Handelshøyskolen BI

GRA 19703 Master Thesis

Thesis Master of Science 100% - W

Predefinert informasjon

Startdato:	09-01-2023 09:00 CET	**Termin:**	202310
Sluttdato:	03-07-2023 12:00 CEST	**Vurderingsform:**	Norsk 6-trinns skala (A-F)
Eksamensform:	T		
Flowkode:	202310||11184||IN00||W||T		
Intern sensor:	(Anonymisert)		

Deltaker

Navn:	Martine Ryan Gulstad og Guro Klevrud

Informasjon fra deltaker

Tittel *:	Exploring consumer willingness to share digital personal data for marketing purposes in a blockchain-based system where consumers control and are incentivized by micropayments for their data
Navn på veileder *:	Ragnhild Silkoset

Inneholder besvarelsen konfidensielt materiale?:	Nei	**Kan besvarelsen offentliggjøres?:**	Ja

Gruppe

Gruppenavn:	(Anonymisert)
Gruppenummer:	115
Andre medlemmer i gruppen:	

Master Thesis

Examination code and name:
GRA 19703

Submission Date:
01.07.2023

Campus:
BI Norwegian Business School, Oslo

Program:
Master of Science in Strategic Marketing Management

Thesis Supervisor:

Ragnhild Silkoset

Title:

Exploring consumer willingness to share digital personal data for marketing purposes in a blockchain-based system where consumers control and are incentivized by micropayments for their data

Acknowledgements

This thesis marks the completion of our Master of Science degrees in Strategic Marketing Management at BI Norwegian Business School. Firstly, we want to express our gratitude to our supervisor, Ragnhild Silkoset, for introducing us to the topic of blockchain technology, and helping us navigate the research of this complex theme. Thank you for generously guiding us through this process, providing us with insights, expertise, and valuable feedback. Secondly, we want to thank all those who contributed to the data collection, and those who responded to the survey.

We would also like to thank our family and friends for supporting and encouraging us during this process. Lastly, we want to thank each other for a great collaboration. Throughout this project, and the past two years, we have motivated each other, learned from each other, and celebrated success together.

Sincerely,

Guro Klevrud & Martine Ryan Gulstad

Abstract

Most webpages today perform some sort of tracking, gathering information about internet users through “cookies”, which are used for creating personalized advertising to target consumers. As regulations are becoming stricter and radical changes such as the “death of third-party cookies” are surfacing, there is currently a need for a new system for marketers to obtain consumer data.

In this thesis we explore one such potential system, facilitated by blockchain technology, where consumers control, and are incentivized by micropayments, for their information. The research focuses on consumers’ general willingness to share digital personal data, and how their willingness to share is affected by their attitude towards, and awareness of, online behavioral advertising and being in control and incentivized by micropayments for their data. We also explore a possible price range and an optimal price for micropayments.

The study was conducted through an online survey with 202 respondents, mainly residing in Norway. Willingness to share digital personal data was measured by a validated framework, categorizing digital personal data in 6 categories. The survey utilized a modified Van Westendorp Price Sensitivity Meter to obtain an acceptable price range for micropayments in exchange for digital personal data.

The results from the study showed that the general willingness to share digital personal data is low, and that consumers’ willingness to share depends on the category of digital personal data. The study suggests that consumers´ attitudes towards personalized advertisements can positively affect their willingness to share information. When given the ability to control their own information collection and use, this study also suggests that consumers are more willing to share all categories of digital personal data. Monetary incentives in the form of micropayments were found to further increase willingness to share in only two categories of digital personal data. This research suggests a provisionally acceptable price range for data, where consumers evaluate NOK 2.55-3.23 as the acceptable price range, and NOK 3.01 as an optimal micropayment for their digital personal data.

Table of Contents

Tables

Figures

1.0 Introduction

In today´s digital world, most webpages perform some sort of tracking, and the average internet user leaves a digital footprint containing vast amounts of information. The major driver for this tracking is the multi-billion dollar industry of advertising, which capitalizes on the opportunities in the digital market to provide personalized and targeted ads to consumers (Kretschmer et al., 2021; Sanchez-Rola et al., 2019). The techniques and regulations for this tracking have evolved and changed with the development of the internet, with the most restrictive regulation to date being the General Data Protection Regulation (GDPR) in the EU. The most common way of tracking a user´s online activity is through "cookies" which involves the placement of small text files on a consumer´s hard drive, which collect useful information, and are subsequently offered back to the web site during repeated visits (Miyazaki, 2008, p. 20). The cookies in themselves are not necessarily a threat to the privacy of the user as many websites rely on these cookies to function properly (Miyazaki, 2008, p. 20). However, numerous websites allow for a third party, such as Meta and Google, to place these cookies on the visitor´s hard drive and track their online behavior, which consumers can perceive as intrusive or overpowering (Aiolfi et al., 2021; Schmidt, 2018).

Online behavioral advertising, also called online behavioral targeting, is "a technique to deliver relevant messages to consumers by basing those messages on an analysis of consumers' online behavior" (Li & Nill, 2020, p. 795). Companies collect data for these analyses based on several dimensions of consumers' online behavior, which is then analyzed and used by companies to deliver personalized messages and advertisements applicable to target customers (Li & Nill, 2020; Nill & Aalberts, 2014). Annually, firms spend a total of $36 billion to capture and leverage customer data, establishing personal data as a financial merit in the data-driven economy (Chua et al., 2021; Columbus, 2014). However, individuals' data disclosure is not rewarded by monetary rewards, but by an exchange for access to digital facilities or content, or by offers of product or service discounts (Chua et al., 2021). This trade-off is often phrased in media as (a variation of): If you're not paying for it, you are the product; A line of thinking dating back to concerns on mass TV advertising in the 1970's (Serra & Weyergraf-Serra,

1980, p. 104). According to Chua et al. (2021), most people are unaware of the financial value of their own data, especially as that value lies in relation to other data, providing data processers the ability to generate new information. Personal data collection increases consumers' data vulnerability, or perceptions of susceptibility to harm, due to unwanted uses of their personal data, such as those that can result from data breaches or identity theft (Martin et al., 2017, p. 36). Martin et al. (2017) theorizes two factors, transparency and control, as suppressors of negative effects of consumers privacy concerns. Transparency of data collection can be defined as consumer awareness of what information they provide to firms, and how that data is collected, used, and shared with other parties (Martin et al., 2017, p. 39). Control in data privacy is the extent to which consumers believe they can manage whether they participate in data sharing, or decide on which types of data they choose to provide (Martin et al., 2017, p. 39).

As regulations are becoming stricter and users are demanding greater levels of privacy protection and control, we are now seeing changes in the way cookies and ad-tracking are being used. In 2020, Google initially announced a phase-out of third-party tracking in 2024, with the reasoning that they do not believe this system meets "rising consumer expectations for privacy" (Bump, 2022). Accompanying this announcement, Apple has disabled all kinds of third-party tracking in Safari as a step to increase user privacy. The company has more recently also launched an iPhone privacy feature called App Tracking Transparency, which further blocks tracking and ads, especially from Facebook (O'Flaherty, 2022, February 19). With the new shift in the direction of less tracking and use of cookies, marketers are wondering how they will operate in the future. Many even believe that in the long run, cookies will die out entirely and be replaced by an alternative which will enhance both privacy and personalization (Patel, 2022). As companies are working on building alternative replacements for data collection, some are seeing the emergence of blockchain technology as a possible, but little researched, solution.

The emerging blockchain technology "holds the potential for societies to become more trustworthy and empowered, increasing visibility, connecting parties, and rewarding individuals for their contributions to transactions. Marketing and advertisement are fundamentally impacted by these changes" (Harvey et al., 2018, p. 5). By tying

micropayments and user behavior together, blockchain technology can allow for companies to bypass ad blocking, and further solve attribution problems of fraudulent or deceptive online marketing activity (Harvey et al., 2018). According to Harvey et al. (2018), marketing teams can use blockchain technology to track their ads and directly measure the impact of marketing efforts down to a per-user metric. Further, enabling consumers to own and voluntarily sell their own data, "individuals will have more control over how they share personal information and how they spend their time interacting with advertisers" (Harvey et al., 2018, p. 5). Previous research on the topic of consumers exchanging their own data on blockchain in the insurance industry has found that people are least likely to share incentivized data of personal online behavior, compared to other data such as driving behavior, heart rate and physical activity (Søndrål & Makin, 2020). However, research has shown that consumer willingness to share data online increases if the consumer experiences a degree of control over the information being shared (Mazurek & Małagocka, 2019). This control can be facilitated by the transparency and security provided by blockchain technology.

The purpose of this study is to provide initial insight into consumer effects of attributes resulting from the potential blockchain based system, which can allow for direct data exchange between consumers and companies. We research consumers´ willingness to share categories of digital personal data, and how being in control of their own data impacts their willingness to share. We also explore the effects of implementing micropayments as an incentive to share personal information, and the compensation level required to facilitate consumer willingness to share digital personal data. We additionally gather information about current consumer awareness about, and attitude towards, the use of data for personalized advertising and how this relates to their willingness to share data. The findings will contribute to the literature on digital consumer behavior, by providing new insights on consumer willingness to share based on a theoretically grounded and updated categorization of digital personal data. Practical contributions for practitioners implementing a blockchain based data sharing system are insights into consumer willingness to share digital personal data, as well as an understanding of how offering control and incentives might impact consumers' willingness to share. Specifically, by identifying which types of data consumers will

be more willing to provide, and which types will demand more effort to obtain, these findings will serve as an initial basis for tailoring data collection efforts to meet consumers' needs for sharing data. Additionally, investigating the monetary value consumers attribute to their personal data gives valuable initial insights into an otherwise little researched topic.

1.1 Research Questions

With basis in the introduction, we formulate the following research questions:

How is consumer willingness to share digital personal data impacted by attitude and awareness towards online behavioral advertising, and affected when offered the ability to control their own data, incentivized by micropayments, in a marketing setting? What is the optimal micropayment to receive in exchange for digital personal data?

1.2 Relevance

The shift in the market towards more consumer privacy and a more restricted use of tracking and information collection, leaves questions about how marketers will operate in the digital world in the coming years, and the potential applications of blockchain technology. Industry professionals and academics state that an early implementation of such blockchain-based data sharing systems will put companies in the best position to benefit from what is believed to be a widespread adoption, which could potentially reinvent their customer relations (Harvey et al., 2018, p. 5).

To potentially implement new systems, it is important to initially research and establish a basis for how consumers will respond and react to shifts in data collection practices. By exploring consumer willingness to exchange digital personal data, we contribute to the literature in this research area by measuring the effect of attributes (control and incentives) that such systems can yield. Further adding to the literature on potential blockchain facilitated data sharing systems, we explore the monetary levels of micropayments consumers require to share digital personal data. These findings will further serve as implications and recommendations on how marketing practitioners can facilitate for data collection and establish an early-adapter position utilizing emerging blockchain technology to increase consumer willingness to share digital personal data.

2.0 Literature Review

This section presents relevant findings from existing literature surrounding the research questions of this study. Firstly, we present previous literature on the topic of willingness to share information. Secondly, we categorize digital personal data based on previous literature, and discuss related work surrounding the variables under which we will study consumer willingness to share information: awareness of, and attitude towards the collection and use of digital personal data, control and incentives. Lastly, we will briefly present and explain the blockchain technology and relevant requirements for the technology to facilitate the proposed system.

2.1 Consumer Willingness to Share Information

The collection and use of consumer data to create individualized marketing communications is one of the fastest growing advances within the marketing field (Hemker et al., 2021, p. 1). With developing restrictive legislations, such as GDPR in the EU and consumer concern regarding collection and use of their personal data, companies will increasingly rely on consumers to willingly share data to facilitate personalized advertising (Hemker et al., 2021, p.3). This study contributes to the body of literature on consumer willingness to share personal data online by providing a categorization of digital personal data and researching willingness to share these categories under different conditions. In this section we discuss existent theory on consumer willingness to share information.

An early theory related to individuals´ willingness to share information, is the theory of Communication Privacy Management (CPM) (Petronio, 2002). This theory describes how individuals believe they have a right to own and regulate access to their private information and make choices on whether to reveal or conceal information, based on criteria they find important (Petronio, 2002, p. 2). CPM is a rules-based theory which focuses on the interplay of disclosing or concealing private information to minimize risks and maximize benefits with communication at its core (Petronio, 2002). Metzger (2007) extends CPM into the e-commerce environment by presenting evidence that online consumers use similar strategies as predicted by CPM, such as information withholding, deception, and to some extent information seeking. In

accordance with CPM, Metzger (2007) found that online consumers may regulate access to different types of personal information based on an assessment of the perceived risk associated with revealing information. The perceived risk was found to be mitigated by the strength of privacy policies as disclosure of information was higher in a strong privacy policy setting compared to a weaker condition (Metzger, 2007, p. 354). This finding suggests that increasing perceived online privacy reduces a consumer´s perceived risk associated with revealing personal information, which in turn has a positive effect on their willingness to share digital personal data. Complimentary findings by Meinert et al. (2006) state that consumers are more willing to share information with online merchants when presented with a strong or moderate privacy policy, compared to no privacy policy.

Contradictory to these findings, researchers have found evidence that the mere existence of privacy notices can produce the so called "bulletproof glass effect", in which the presence of a privacy notice paradoxically can create a sense of vulnerability in consumers as they are reminded of the possible dangers of sharing their data with a company (Brough et al., 2019, p. 40). Brough et al. (2019) find that the assurance can function as a warning, leading to risk avoiding behaviors. In line with CPM, these risk avoiding behaviors include lower willingness to share personal information (Brough et al., 2019, p. 41).

The dichotomy of findings regarding privacy policies can partially be explained by the Privacy Calculus Theory introduced by Laufer & Wolfe (1977, as cited in Culnan & Bies, 2003). This model explains that consumers behave according to a cost-benefit analysis. When asked to share information, the benefit consumers receive for disclosing that information should exceed the perceived risk that accompanies the information disclosure (Culnan & Bies, 2003, p. 327). To summarize, the presence of a privacy policy functions as a moderator of perceived risk, which can potentially reduce or increase consumer perceived risk.

As a privacy policy alone is not sufficient as a singular moderator of consumer perceived risk in sharing digital personal data, previous literature suggests other variables which can decrease perceived risk, and thereby increase willingness to share

data. Phelps et al. (2000) points to two factors as most important, being the “type of information collected” and “the amount of control consumers have over subsequent dissemination” (p. 38). In addition, consumers´ awareness of, and attitudes towards, data collection and use is suggested to determine consumer behavior, indicating that this could have an effect on their willingness to share digital personal data (Dehling et al., 2019; Friestad & Wright, 1994). This research adds to the body of literature on the topic of consumer willingness to share, by studying the effects that type of data, awareness of and attitude toward data collection and use, control and incentives have on consumer´s willingness to share digital personal data for marketing purposes.

2.1.1 Categories of Digital Personal Data

Establishing categories of digital personal data can create a mutual understanding of what personal data “is” between consumers and companies, which can increase transparency in the handling of personal data (Chua et al., 2021, p. 3). Further, by categorizing data, consumers can gain more information about which data is collected and processed, enhancing their confidence in disclosing their data to companies (Chua et al., 2021, p. 4). Previous research suggest that there are differences in willingness to share depending on the type of information respondents are asked to provide (Chua et al., 2021; Meinert et al., 2006). Meinert et al. (2006) explains that there is inherent risk associated with different types of personal information, and therefore also a difference in willingness to share different types of information among consumers. A large body of research has been conducted on data privacy and personal data as a singular concept, whereas a sparse amount of research has provided an in-depth categorization of personal data. In this section we present previous research on the topic of consumer willingness to share categories of digital personal data and present an updated categorization of digital personal data types.

Phelps et al. (2000), were one of the first to identify and scale consumers´ individual willingness to share information in a modern commerce context. This measurement scale consists of 16 items in 5 categories, and willingness to share is measured by consumer evaluation of each item on a 4-point Likert scale. In line with societal and technological developments, this measurement scale has served as basis for later

research on consumer willingness to share personal information in digital settings. Adapting the scale from Phelps et al. (2000), Gupta et al. (2010) extended the number of items to additionally measure privacy and security protection constructs, and found significant cultural differences in consumers' willingness to share personal information.

By conducting a survey where adolescents were asked to rate their willingness to share 14 categories of digital personal data on a website, Heirman et al. (2013) confirmed a multidimensional construct of willingness to share data, consisting of 4 overall categories of digital personal data. They further found that respondents' trust and disposition to trust in the website predicted their willingness to share, and that their risk perception affected their willingness to share (Heirman et al., 2013). Milne et al. (2017) further expanded on the literature on willingness to share, researching the impact of consumer concern regarding information privacy. Building on the initial categorization of Phelps et al. (2000), they conducted a large study where 52 types of personal data types were analyzed along perceived risk, overall sensitivity regarding the information, and consumer willingness to provide it. They found an overall categorization of 4 personal data types (Milne et al., 2017, p. 133). Robinson (2017) examined how demographic variables affect consumer willingness to share personal information. The study utilized 17 items of personal data, and analysis showed a significant difference in willingness to share both within and between nationalities (Robinson, 2017, p. 569). Knowledge of ecommerce experience was also found to be an important predictor of consumers' willingness to share, as well as perceived risk of sharing (Robinson, 2017, p. 576).

Chua et al. (2021), further extended the original categorization of Phelps et al. (2000), to account for technological developments of digital data collection. The study provided an in-depth data categorization with systematic validation, deriving a total of 6 categories that together compose digital personal data (Chua et al., 2021, p. 5). These categories are labeled as Social-Economic, Medical Health, Lifestyle-Behavior, Tracking, Authenticating and Financial. Their findings show that demographic factors such as age, gender and working industry to some degree affect consumers' privacy concern and intention to share personal information (Chua et al., 2021, p. 1).

Table 1 presents a classification of digital personal data based on the previous research of Chua et al. (2021), Gupta et al. (2010), Heirman et al. (2013), Milne et al. (2017), Phelps et al. (2000), and Robinson (2017). Each dimension is sorted based on the validated categories of Chua et al (2021).

Table 1. Classification of Digital Personal Data Categories

	Social-Economic	Medical Health	Lifestyle-Behavior	Tracking	Authenticating	Financial
Phelps et al. (2000)	Demographic characteristics		Lifestyle characteristics Shopping & Purchasing habits		Personal identifiers	Financial info
Gupta et al. (2010)	Demographic data	Medical history	Media habits Lifestyle data	Home address Work address	Name Email address Date of birth Home phone number Work phone number	Credit card details Financial information
Heirman et al. (2013)			Profile information	Geographical data	Identity data Contact data	
Milne et al. (2017)	Basic demographics		Personal preferences Community interaction	Contact info	Secure identifiers	Financial information
Robinson (2017)	Age Marital status	Medical history		Home address Work address	Name Home phone number Work phone number Email address Date of birth Twitter handle Facebook profile Skype username	Credit card number Annual income Credit history Paypal account
Chua et al. (2021)	Social-economic	Medical health	Lifestyle-behavior	Tracking	Authenticating	Financial

A category overview for this study is presented below in Table 2. The overall categorization labels are derived from the study of Chua et al., (2021) with a slight change to the category name “Social-Economic” which in this study is referred to as “Socio-Demographic” to better capture previous categorizations and its intended measure.

Table 2. Category Characteristics of Digital Personal Data (Chua et al., 2021)

Category	Characteristics
Socio-Demographic	Information that describes an individual´s general demographics and physical characteristics, as well as their education and career.
Medical Health	Information regarding individuals' genetic data, medical and mental health, including health records, prescriptions, and medication history.
Lifestyle-Behavior	Information describing an individual´s lifestyle characteristics and behavior such as personal beliefs, preferences, relationships, and media habits.
Tracking	Information that can be used to locate and/or contact an individual, such as their physical address, IP-address, and contact information.
Authenticating	Information that can be used to verify the identity of an individual, such as their full name, passwords, fingerprint, and face-ID.
Financial	Information regarding individuals' financial accounts and transactions, such as their income, purchase history, credit card number, and account details.

Applying the original categorization framework, Phelps et al. (2000) found significant difference in consumer willingness to share personal information across categories and items. Categorical mean evaluations of willingness to share were highest for demographic and lifestyle information, followed by purchase-related information. Consumers were least willing to provide personal identifiers and financial information (Phelps et al., 2000, p. 34). Similar results were reported by Chua et al. (2021), who found that consumers' highest privacy concern was personally authenticating information, followed by financial information. These categories were also rated with the lowest level of disclosure intention by the respondents (Chua et al., 2021, p. 10). The categories rated with the least privacy concern were Lifestyle-Behavior and Social-Economic, which consequently are the most likely categories for disclosure intention of personal information (Chua et al., 2021, p. 12). However, they found no significant difference in between the ratings of lifestyle-behavior and social-economic, tracking and medical health, as well as finance and authenticating categories.

This study contributes to the literature by applying a technologically updated categorization framework rooted in previous research on consumer willingness to share. Although consumers' willingness to share personal information has transformed over time, Milne and Bahl (2010) states that established norms in the market place largely determines consumer willingness to share. Based on presented findings from previous literature, we expect to see a similar relationship between categories of

personal data and willingness to share within this framework, and therefore formulate the following hypothesis:

H1: *Consumers' willingness to share personal data for marketing purposes differ between categories of digital personal data*

2.1.2 Consumer Awareness and Attitude Towards Online Behavioral Advertising

As consumer data is used by companies to target consumers more accurately through online behavioral advertising, an interesting relationship to explore is the one between consumer awareness and attitude towards online behavioral advertising and willingness to share digital personal data. Our study contributes to the research on willingness to share data in a marketing perspective by studying how the level of awareness of online behavioral advertising and attitude towards personalized advertising influences consumers´ willingness to share digital personal data for marketing purposes.

The "Persuasion Knowledge Model" by Friestad & Wright (1994) explains how consumers form attitudes when exposed to advertising. According to the model, consumers accumulate knowledge about persuasion techniques as they are exposed to these techniques, both through advertising but also in other aspects, throughout life. The knowledge they inhibit will determine how their attitudes are formed and how they behave when they are exposed to persuasion attempts in advertising (Friestad & Wright, 1994). Recognizing a persuasion tactic in an advertisement can lead to what Friestad and Wright (1994) call "change of meaning". When the "change of meaning" occurs, a consumer who initially did not generate any particular feelings toward the advertisement or its sender, recognizes the persuasion tactic, which activates a coping behavior in the consumer (Friestad & Wright, 1994). These coping behaviors can include resistance and avoidance, but also potentially more positive behaviors if the persuasion tactic or marketing message aligns with the consumers´ goals (Friestad & Wright, 1994). Applying this model to the use of personalization as a persuasion tactic suggests that the knowledge consumers inhibit about online behavioral advertising and whether they recognize personalization as a persuasion tactic, will determine which attitudes they form towards the advertisements.

The persuasion knowledge model can be linked to the findings of Dehling et al. (2019), in their study of how consumers perceive online behavioral advertising. They suggest that most consumers are generally aware of online behavioral advertising and possess different degrees of knowledge about the technology. Through interviews with 13 people from different countries in Europe and China, they found that all interviewees could recall having seen ads depicting something they had previously searched for, however they were sometimes not sure whether it was simply a coincidence or clever targeting (Dehling et al., 2019). Among the interviewees, most also inhabited an understanding of how they are tracked and what types of information are being collected, but had less knowledge about how online behavioral advertising works from a technical aspect (Dehling et al., 2019). In the consumer online behavioral advertising perception model, Dehling et al. (2019) postulate, in line with the persuasion knowledge model, that consumers´ attitudes toward online behavioral advertising depend on their awareness and knowledge. Consumers with higher perceived awareness and knowledge reported being less concerned about online behavioral advertising because of the knowledge they believed they possessed (Dehling et al., 2019). They reported feeling less insecure and more accepting when confronted with personalized advertisements. Consumers with more limited knowledge, on the other hand, reported being more concerned about online behavioral advertising (Dehling et al., 2019). They also suggest that consumers´ attitudes towards personalized advertisements are dynamic and evolve as they are being confronted with the advertisements. As long as consumers do not get annoyed or experience their personal threshold to be violated, they generally accept online behavioral advertising and often also see value in it (Dehling et al., 2019).

Other previous studies have also found personalized ads to be both favorable for consumers and have a positive effect on consumer response rates. The benefits of personalized ads for the consumer are suggested to be more relevant information, better preference matches, better products, better service and better experience (Vesanen, 2007, p. 414). Out of these, Strycharz et al. (2019) found relevance to be the most prevalent self-reported benefit of personalization among consumers. Relevance is defined as the extent to which a consumer believes a concept to be self-related or in

some way instrumental to satisfying their interests, needs or goals (Celsi & Olson, 1988, p. 211). Consumers experience that relevant personalized ads give them offers they might actually be interested in (Strycharz et al., 2019, p. 59). Some consumers are even interested in preselecting categories of ads that are of interest to them, to receive even more relevant advertisements (Dehling et al., 2019). In addition to relevance, personalized ads are also found to be convenient for fulfilling consumers´ needs (Strycharz et al., 2019, p. 59). Personalized ads help consumers be more efficient online, make surfing more effortless and remind consumers to buy products they need (Strycharz et al., 2019, p. 59). Effects of personalization on consumer response rates have also been measured, including in an experiment measuring clicks on personalized ads versus non-personalized ads by Tam & Ho (2006). Personalized ads were found to have a significantly higher click-through-rate compared to non-personalized ads (Tam & Ho, 2006, p. 880-881). It has also been found that relevance has a positive mediation effect of personalization on consumer response rates (De Keyzer et al., 2015, p. 130). These findings suggest that consumers find personalized ads helpful, convenient, and more engaging compared to non-personalized ads.

Although it has been found that response rates improve with greater ad personalization, high personalization can also lead to consumer discomfort and suspicion, resulting in lower response rates (Aguirre et al., 2015, p. 35). This phenomenon is called the personalization paradox and research has found evidence of this paradox with regards to information collection (Aguirre et al., 2015). When information to provide personalized services is overtly collected, click-through intentions increase among consumers. However, when information is collected covertly, consumers feel more vulnerable when detecting that their information has been collected without consent, activating coping behaviors in the consumer, thereby decreasing click-through intentions (Aguirre et al., 2015, p. 41). Consumers believe that they own their personal information and will therefore react negatively to advertising using this information unless consumers have given their explicit permission (Aguirre et al., 2015, p. 44). The personalization paradox therefore suggests that consumers are susceptible to personalized advertisements, but only when they are aware that this information has been consensually accessed.

Previous research suggests that personalized advertisements often are favorable to consumers, particularly to consumers who are aware and knowledgeable about online behavioral advertising, and that positive attitudes towards personalized advertisements increases positive coping behaviors such as click-through rates (Dehling et al., 2019; Friestad & Wright, 1994; Tam & Ho, 2006). We contribute to the body of literature by researching the relationship between consumers´ awareness of online behavioral advertising and attitude toward personalized advertisements, and the potential coping behavior of willingness to share digital personal data. In line with the persuasion knowledge model, we hypothesize that consumers who recognize personalized advertisements as useful will engage in positive coping behaviors such as increased willingness to share data. We predict that high consumer awareness of how digital personal data is collected and used decreases discomfort and suspicion among consumers, and increase their evaluations of the usefulness of personalized ads, making these consumers more inclined to share their information for marketing purposes. Thus, we formulate the following hypothesis for this study:

H2: *Consumer awareness of and attitude towards online behavioral advertising has a positive effect on consumers' willingness to share digital personal data with companies for marketing purposes*

2.1.3 Effect of Control on Consumer Willingness to Share Data

Previous literature has found consumer perceived control to have a suppressing effect on privacy concerns in data collection (Martin et al., 2017, p. 36). The body of research on constructs of consumer privacy concerns is quite extensive, however past research has largely focused on consumer reservations and privacy concerns, capturing the barriers, rather than facilitators, of consumer willingness to share digital personal information. One central exception of this is the early research by Phelps et al. (2000), exploring trade-offs consumers are willing to make when they exchange personal data. The findings of this study indicate that higher consumer perceived control of personal data can reduce overall privacy concerns (Phelps et al., 2000 p. 39).

In recent research, control over personal data has been defined as consumers' right and ability to decide which personal information should be collected and made available to

others, and the ability to decide when the information should be deleted (Shulman & Meyer, 2022, p. 40596). Building on these premises, Shulman & Meyer (2022) expand the definition of control to further include knowledge on what the consequences of information disclosure or deletion action entail. Offering consumers control of their own data can lead to a higher rate of advertising accept and interest and reduced negative effects of privacy concerns on intention to engage with a website (Phelps et al., 2000; Taylor et al., 2009). Reversely, Baek & Morimoto (2012) state that a lack of choice and control can lead to advertising resistance. By offering consumers control, they experience having a voice in initiating the advertising they are exposed to. This finding is supported by Dehling et al. (2019), stating that to avoid feeling manipulated, consumers should be given more control over the ads they are confronted with. Further, control and transparency can function as suppressors to synergistically mitigate consumers´ feelings of violation, and further enhance trust towards the company collecting and processing the data (Martin et al., 2017, p. 52).

Previous research on the direct effect of control on consumer willingness to share personal information is largely limited, although a few studies have provided relevant findings. In a large study on consumer willingness to share information with online advertisers, Leon et al. (2013) found that providing consumers access to review their data did not significantly affect their willingness to share it, with a slight majority stating that they would be more willing to share (48%) compared to equally willing (41%). However, when presented with a hypothetical online plugin which could allow participants to control collected information, they found that participants were more willing to share anonymous (84% of participants) and personally identifiable (74% of participants) information with advertisers (Leon et al., 2013, p. 9). They suggest further research on the topic is needed. In an experiment setting, Weydert et al. (2019) introduced control over data use as “active transparency”, the ability to control what the company uses the collected data for and who this data is sold to. They found that control can be an effective way to increase consumers´ willingness to share data, as increasing control can be an effective strategy to make consumers more comfortable sharing digital personal data (Weydert et al., 2019, p. 6).

Considering previous studies on the effect of control on willingness to share personal information is limited, we contribute to the body of research by testing the categorical framework of willingness to share digital personal data under a control condition. Although Leon et al. (2013) suggest that control has minimal impact on consumer willingness to share data, other presented literature find control to be a mitigator of privacy concern and risk related to data collection. As consumer willingness to share data has been found to be highly dependent on their perception of related risk, we predict that in a marketing context, consumers´ willingness to share digital personal data increases when they are given control over their own data. We therefore formulate the following hypothesis:

H3: *Having control over own data positively affects consumers´ willingness to share all categories of digital personal data for marketing purposes*

2.1.4 Effect of Incentives on Consumer Willingness to Share Data

Previous literature on consumer willingness to share digital personal data has been interested in the effect of incentives or compensation for sharing information, and has found differences in effects based on the type of incentive used and the type of data requested (Ackermann et al., 2022; Gabisch & Milne, 2014). As this is still a somewhat unexplored topic, we contribute to the literature by studying the effects of incentives, specifically monetary incentives, on consumer willingness to share the previously established categories of digital personal data for marketing purposes, in a setting where we also account for the effect of consumer perceived control.

The previously presented Privacy Calculus Theory suggest the possibility that incentives can increase consumer willingness to share digital personal data, if the benefits (incentives) are perceived to be greater than the risk of sharing (Culnan & Bies, 2003, p. 327). In line with this theory, previous studies suggest that incentives can have a positive effect on consumers' willingness to share digital personal data. Gabisch and Milne (2014) found in their study that consumers are willing to share their ownership rights of data with marketers in exchange for benefits on the internet. Particularly for data regarded as sensitive, compensation is found to decrease consumers' ownership beliefs and control expectations, and therefore increase their willingness to share digital

personal data (Gabisch & Milne, 2014, p. 19). This study does not measure the degree to which consumers initially believe that they are in control of their own data, but the degree to which they expect to be in control after exchanging data for monetary incentives. Ackermann et al. (2022) compared the effect of five different forms of incentives (or compensation) on willingness to share different data points. In the study, they created a model which predicted that financial compensation would lead to the highest predicted willingness to share in all types of data, whereas virtual compensation, such as digital reward points, predicted the lowest willingness to share, even lower than no compensation at all (Ackermann et al., 2022). Benndorf & Normann (2018) adds to this line of findings with their study, in which 83% of participants in their experiment were willing to sell their personal data for 5 euros, while only 12% of their survey participants were willing to hypothetically sell their information without receiving any incentive upfront.

On the other hand, Weydert et al. (2019) has found monetary compensation to have a potentially negative, although small, effect on consumer willingness to share digital personal data. They found that when offered a high amount of money (USD 67 per year) for their data, consumers' willingness to share decreased for data with low perceived sensitivity among promotion-oriented people. This is an interesting finding, as it suggests there exists a threshold for the monetary level for which incentives increase consumers' willingness to share personal data. This finding also suggests a difference in the effects of incentive effects on willingness to share different types of data, in line with Gabisch & Milne (2014). Weydert et al. (2019) explains their findings by suggesting that being offered monetary compensation for their information activates a signaling effect through which the monetary value offered signals the potential privacy protection loss for the consumer, thereby reducing their willingness to share. As low sensitivity data is generally associated with a low risk when shared, placing a high monetary value on this type of data might signal a higher risk than initially perceived (Weydert et al., 2020).

The findings regarding incentives generally suggest a positive effect of incentives on consumers' willingness to share digital personal data. Based on the presented findings, we predict similar results of increased willingness to share data, when respondents are

offered monetary incentives in this study. Expanding on the work of Weydert et al., (2019) and Gabisch and Milne (2014), we expect to see a difference in the effect size of incentives on consumer willingness to share, depending on the category of digital personal data. We formulate the following hypothesis:

H4*: Monetary incentives positively affect consumers´ willingness to share all categories of digital personal data for marketing purposes.*

The aforementioned study by Gabisch and Milne (2014) researching the presence of compensation, used a USD 50 check as compensation for filling out a customer satisfactory form on a website. In the current study, we propose owning and controlling digital personal data on blockchain for safer and more effective data sharing, compared to filling out online forms or giving consent to data collection each time a website is visited. As this technology allows for direct transfer of data from the consumer to the company, we suggest micropayments as an efficient payment method to implement in this solution.

Micropayments are generally used for the payment of low amount transactions, and can be used in online streaming, software purchasing, online advertising or accessing information. A micropayment solution can be used to pay an amount per click on a website, or per minute a song or video is streamed online (Micali & Rivest, 2002, p. 2). With the development of the Internet of Things era, an important enabler would be the automatic payments between devices without human interaction (Lundqvist et al., 2017, p. 1). As of now, the implementation of micropayments is very topical, and there are few implemented and empirically tried systems.

A micropayment system needs to satisfy a set of criteria depending on system requirements and the network environment as explained by Kiyomoto et al. (2004): Electronic coins cannot be forged or re-used, and there needs to be protection against double spending in the system (*Security).* Electronic coins are almost universally accepted (*Acceptability),* and the system needs to decide to which extent the payer is anonymous (*Anonymity).* The system also needs to be robust in terms of network failures (*Atomicity)*. Lastly, a user has to be able to spend electronic coins they have received without having to access them through a bank (*Transferability),* and payers

should be able to make changes themselves (*Divisibility*) (Kiyomoto et al., 2004, p. 871). The problems related to the traditional use of micropayments have been high transaction costs and the need to share credit-card information with a device, which in turn shares this information with other devices when performing the payment (Lundqvist et al., 2017, p. 1). It has therefore been difficult to implement an effective autonomous micropayment solution. A proposed solution to the limitations of traditional micropayments is the blockchain technology (Lundqvist et al., 2017). . However, more research on how it can be implemented effectively is needed.

There is currently a gap in the theory regarding specific valuation of data shared by consumers, especially from a consumer perspective, or in the proposed context of exchanging digital personal data on blockchain through micropayments. Moreover, the existing research scarcely control for an upper monetary limit or frame the potential value of micropayments. Most previous studies have also used relatively high (one-time) payments such as USD 50 or USD 67, values initiated by the researchers rather than the consumers themselves (Gabisch & Milne, 2014; Weydert et al., 2020). One of few studies exploring the potential price tag put on digital personal data by consumers, is a study from 2013 on Spanish internet users, by Carrascal et al. (2013). This study found that users generally value their personally identifiable information related to browsing activity to about 7 Euros (USD 10 at the time) (Carrascal et al., 2013). In this study we add to the limited body of research on consumer valuation of digital personal data by introducing a monetary range and exploring the research question:

What is the optimal micropayment to receive in exchange for digital personal data?

2.2 Blockchain Technology

In this study, we introduce and explore a system that enables control and incentivization of consumer data. To effectively and securely facilitate such a system, we propose blockchain technology as the underlying digital infrastructure. Blockchain technology may be eligible for this system, as it encompasses possibilities for storing and controlling data across industries (Harvey et al., 2018, p. 2).

The first ideas of blockchains emerged in the 1990s and the technology was utilized in the development of electronic cash in 2008 (Yaga et al., 2018). Bitcoin is today

considered the first of several later applications of the blockchain. A blockchain is a digital distributed ledger that is tamper proof and tamper evident. The ledger includes all activity performed by the blockchain´s participants (Saberi et al., 2019, p. 2118). When an agent creates a new transaction in a blockchain, the transaction is accepted by the pre-specified and approved nodes in the chain and is added to the chain as a new block (Saberi et al., 2019, p. 2118). Blockchains create honest systems that self-correct, meaning that the consensus algorithm enforces preset rules (Laurence, 2019, p. 13). The blockchain technology can therefore ensure safe transactions without the need for a third party.

Laurence (2019) explains the structure of blockchains as following: Each blockchain is individually structured, and consists of three core elements: blocks, chains, and network. Blocks are lists of transactions recorded into a ledger over a given period. The chain can be described as a hash that links individual blocks to each other, chaining them together. This process is what secures and ensures the information within the blockchain. The hash can be described as fingerprints of the data which lock blocks in order and time, creating a one-way function that is impossible to decrypt. The third component is the network, which is composed of "full nodes". Nodes are devices, such as computers, which hold complete records of all transactions of that blockchain. This can be described as securing the network by running an algorithm on a computer (Laurence, 2019).

Trust is an important component in storing sensitive information on a blockchain. Blockchains establish trust in several ways. Two of the more well-known are proof-of-work and proof-of-stake (Laurence, 2019, p. 10). Proof-of-work blockchains require miners to provide a history of all transactions they have made to be allowed to participate in the network, while proof-of-stake blockchains require participants to "stake" some cryptocurrency that will be sanctioned if they are caught acting dishonest (Laurence, 2019, p. 10). The elimination of a third party also leads to increased trust in a transaction, as explained by Laurence (2019): Data stored off-chain relies on a single database which is controlled by an entity. Not only does this database become more vulnerable as it relies on a single point of failure, but it also requires that the entity controlling the data is trusted by others for its content to be considered credible. Storing

data on the blockchain, however, is safer as it is stored on a network of independent users, and the computers that make up the network are in more than one location (Laurence, 2019). Blockchains also do not require trust in a central authority, which entails prominent implications, particularly in countries with generally lower trust in authorities (Laurence, 2019).

In terms of personal data storing, it is important to distinguish between two types of blockchains, namely public and private. A blockchain is public when every participant in the network can read it and carry out a transaction using it, but also when everyone can participate in verifying it to reach consensus (Chowdhury et al., 2018). Because everyone in the network has to reach consensus on the state of transactions, public blockchains have limited transaction processing rates (Yang et al., 2020, p. 2). A blockchain can also be private (or semi-private) if only a specified number of authorized participants can carry out the consensus process (Chowdhury et al., 2018). A private blockchain can reach consensus faster and can therefore carry out several transactions in a matter of seconds (Yang et al., 2020, p. 2). For personal data storing and handling, either type of blockchain can be applied.

2.2.1 Privacy Requirements for Blockchain Based Systems

Any system that collects personal data must comply with privacy and data protection requirements (The World Bank, 2019). We therefore consider it necessary to discuss privacy requirements for blockchain. For the technology to protect privacy, it needs to satisfy two requirements: 1) The links between transactions should not be visible, and 2) the content of the transaction is only known to the parties involved in the transaction (Feng et al., 2019, p. 48). Another requirement for privacy stated by GDPR is the possibility of erasing data when requested by the user, which raises problems in the blockchain as it is, in its nature, immutable (Bernabe et al., 2019, p. 164914). This GDPR regulation is not applicable to fully anonymous data, however data on-chain is encrypted and therefore pseudonymous rather than anonymous (Bernabe et al., 2019, pp. 164914-164915). More recently, Kuhn (2022) describes in a whitepaper a data structure which he refers to as a data block matrix. This structure supports integrity protection while also allowing for deletion of records. He suggests this structure to be

incorporated into systems currently using blockchains, to further strengthen integrity protection and solve the issues related to erasure (Kuhn, 2022).

2.3 Research Framework

This study aims to explore a potential blockchain-based system where consumers control their own data and are incentivized by micropayments for sharing digital personal data with companies for marketing purposes. Through this research we add to the body of literature on consumer willingness to share personal information, by measuring effects of awareness and attitude, control and incentivization. The conceptual framework of this research is visualized in Figure 1, and an overview of the hypotheses is presented in Table 3.

Figure 1. Research Framework

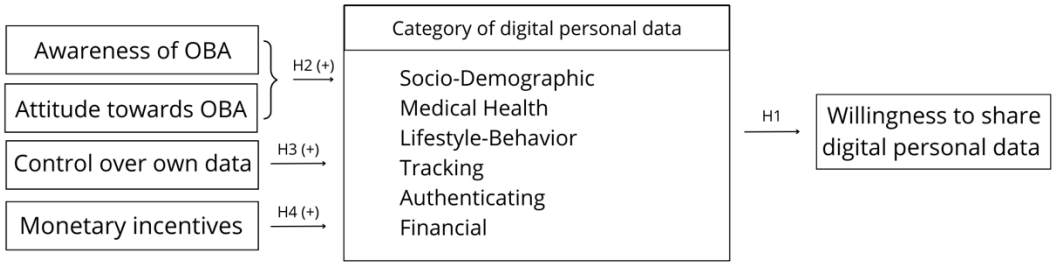


Table 3. Overview of Hypotheses

Hypotheses	Hypothesized effect
H_1: *Consumers' willingness to share personal data for marketing purposes differ between categories of digital personal data*	+/-
H_2: *Consumer awareness of and attitude toward online behavioral advertising has a positive effect on consumers' willingness to share digital personal data with companies for marketing purposes*	+
H_3: *Having control over own data positively affects consumers´ willingness to share all categories of digital personal data for marketing purposes*	+
H_4: *Monetary incentives positively affect consumers´ willingness to share all categories of digital personal data for marketing purposes.*	+

The conceptual research framework for this study (Figure 1) illustrates the following: (H1) How consumer willingness to share depends on the category of digital personal data, (H2) how consumer awareness and attitude toward online behavioral advertising (OBA) affects willingness to share digital personal data, (H3) how offering consumers control over own data and (H4) how monetary incentives affects their willingness to share digital personal data. Hypothesized directional effects of independent factors are illustrated with "+" or "-".

3.0 Research Method

Our study applies a descriptive research method where we use a survey to uncover consumer characteristics through further analyses. In the following sections, we describe how we collected the data used to test the hypotheses and explore the research questions.

3.1 Survey Design

We conducted quantitative research based on structured data collection through a cross-sectional survey, from which collected data serve as a basis for analyses and hypothesis testing. A survey is a structured questionnaire used to obtain specific information from a sample of a population, and is one of the most common methods of primary data collection in marketing research (Malhotra, 2020, p. 193). The advantages of data collection by survey in marketing research is that it is easy to administer, and the obtained data is relatively straightforward to analyze. Further, the obtained answers are reliable and less variable because responses are limited to the alternatives stated in the survey (Malhotra, 2020, p. 193).

A limitation to this method is the wording of questions, which is crucial to capture the concept intended to measure. In addition, respondents might be unable or unwilling to provide the desired information, which they are unable to report due to the nature of survey designs (Malhotra, 2020, p. 193). It is important to consider these limitations when creating the survey, in effort to minimize them. The survey used in this research was self-administered by participants online. It was comprised of a statement of informed consent, followed by six blocks separating each step of the data collection which we present below:

(1) Consumer Awareness, Control and Attitude towards online behavioral advertising: Knowledge and awareness are important factors of a consumer´s attitude formation when presented with advertisements, and the attitude formation is important for the following consumer behavior (Dehling et al., 2019; Friestad & Wright, 1994). Degree of experienced control is also suggested as an important factor in attitude formation toward advertising (Baek & Morimoto, 2012; Dehling et al., 2019; Phelps et al., 2000; Taylor et al., 2009). The first block of the survey therefore consisted of a measure of consumer self-reported awareness of online behavioral advertising, their attitude towards personalized advertising, and whether they believe they are in control of the collection and use of their digital personal data. The respondents were asked to rate the degree to which they agreed with a series of statements on a 5-point Likert scale, where 1 is "Strongly disagree" and 5 is "Strongly agree". We included two negatively worded statements for measuring feeling of control and attitude, to capture a broader domain of the construct and combat response bias. The display order of the questions in this block was random, to combat the question order effect, which is a type of response bias (Schuman & Presser, 1996).

(2) Willingness to Share Digital Personal Data: The complete framework for this study is based on the 6 operationalized categories of digital personal data, from the frameworks of Chua et al. (2021), Gupta et al. (2010), Heirman et al. (2013), Milne et al. (2017), Phelps et al. (2000), and Robinson (2017). Consumer willingness to share digital personal data was measured by having respondents indicate their willingness to share 17 items of digital personal data, mainly derived from the data collection process of Chua et al. (2021). The items and their corresponding categories are presented in Appendix 1. Willingness to share digital personal data was indicated on a 5-point Likert scale, where 1 is "Unwilling" and 5 is "Willing".

(3) Control: Control has been suggested to have an impact on consumer willingness to share both directly and through mitigating privacy concerns (Leon et al., 2013; Martin et al., 2017; Phelps et al., 2000; Weydert et al., 2020). To measure the effect of control on consumer willingness to share digital personal data, respondents were presented with a scenario and example, where new technology facilitates consumer control and direct data transfer between consumers and companies. Under this condition, which we

will call the control condition, respondents were again asked to indicate their willingness to share each item of digital personal data on the 5-point Likert scale.

(4) Monetary Incentive: In our research, we aim to provide an indication of the monetary value consumers assign their digital personal data. For this, we adapted and applied Van Westendorp's Price Sensitivity Meter, which is a direct technique used for researching pricing sensitivity (Ceylana et al., 2014, p. 5). This model, first introduced by the Dutch economist Peter H. van Westendorp in 1976, is a heuristic procedure of gathering data on acceptable price for a product innovation, aiming to indicate an optimal price (Lipovetsky, 2006). The assumption of this model is that consumers cannot state one perfect price for a product, but can instead indicate an acceptable price range (Ceylana et al., 2014, p. 3). The model consists of 4 questions (from Ceylana et al., 2014, p. 3):

1. At what price would you consider this product to be so expensive that you would not consider buying it?
2. At what price would you consider the price of this product so low that you would question its quality?
3. At what price would you consider this product starting to get expensive – not out of the question, but you would need to give it some thought before buying it?
4. At what price would you consider this product to be a bargain – a great buy for the money?

For this research, we used the Van Westendorp model as a basis, and modified the questions so that respondents indicated a range of acceptable payments for sharing, rather than price for buying. Resultantly, our model contains the following 4 questions:

1. At what price would you consider the payment to be so low that sharing your information would not be worth it?
2. At what price do you consider the payment for sharing your information to be so high you become suspicious of the buyer´s intentions?
3. At what price would you consider the payment to be low but still high enough so that you would start considering sharing your information?

4. At what price would you consider the payment to be a good deal for sharing your information without becoming suspicious of the buyer´s intentions?

To measure the monetary incentive level required for sharing digital personal data, respondents were introduced to a hypothetical, yet plausible situation. In this scenario, sharing data with a music streaming company would be rewarded with a micropayment. Micropayments are in the literature generally defined as "small payments", but there does not seem to be an agreement on the exact amount that qualifies as a micropayment (Reddy et al., 2010; Rivest, 2004). Herzberg (2003) states that the threshold for a micropayment is the minimal transaction fee for payment by credit card, which at the time was 20 cent. In the early work by Rivest (1997), electronic lottery tickets with a face value of USD 10 and 1/1000 chance of winning, allowed the buyer to pay the vendor 1 cent by giving him such a ticket. The upper limit for a micropayment is not defined.

Implementing the Van Westendorp model to explore micropayment incentive levels, we provided respondents with an incentive range within the bounds of previous research on micropayments. In the example situation, respondents were asked to select four price points within the range of 0-5 Norwegian Kroner. At the time of creating and distributing the survey, the value of NOK 1 equaled USD .096. For the convenience of international respondents, we rounded this up to USD .10, stating in the survey that NOK 5 equaled approximately USD .50.

Continuing the scenario of receiving a monetary incentive for sharing digital personal data, which we will call the incentive condition, respondents again indicated their willingness to share each category of digital personal data on the 5-point Likert scale.

(6) Demographic: In the last block, respondents were asked to provide general demographic information, including gender, age, occupation, and country of residence (Hughes et al., 2016). The final question was an open field text entry which provided respondents an opportunity to elaborate or comment on the survey.

A complete overview of the survey structure and the questionnaire in full is attached in Appendix 2. and 3., respectively.

3.2 Sample Participants

As this study encompasses anyone with regular access to the internet, we aimed to collect answers representative for the general population to strengthen external validity and make the findings generalizable. We used a single cross-sectional design for the study. For legal and ethical reasons, we only included respondents older than 18. To calculate an appropriate sample size, we determine a 95% confidence level, a standard deviation of .5, and a margin of error of 5% to be appropriate.

$$Sample\ Size = \frac{Z^2 * variance}{error^2}$$

This gives us the calculated minimum sample size:

$$Sample\ Size = \frac{1.96^2 * 0.5^2}{0.05^2}$$

The minimum sample size required to ensure generalizability is therefore 384. To ensure a representative sample of the final survey, we would have preferred to recruit participants by simple random sampling. However, this method was not feasible because of limitations in resources and time. Additionally, the population is large, making it difficult to assign every participant the same probability for answering the survey. Therefore, we recruited participants by non-probability convenience and snowball sampling, as these methods were attainable in terms of the constraints of this research project. This is a limitation in our research method, which might affect the representability and generalizability of findings.

3.3 Dissemination

The survey was created and distributed digitally using the online survey tool Qualtrics. Before distribution, the survey was pilot tested on a small sample within our network to check for potential uncertainties and collective understanding. Test-respondents were asked to measure their time spent taking the survey, so we could provide respondents with a verified time frame for completing the survey. After completion, test-respondents provided feedback on individual questions and the survey as a whole. Based on the responses and feedback, we made slight changes to question formulations and examples, to ensure that they were clear and easy to understand.

The survey was distributed by an anonymous link on Facebook, Instagram, and LinkedIn. In addition to reaching our own networks, we also connected with industry professionals who shared the survey on their private and business platforms on LinkedIn and by email within their organizations. The survey was open for participation for a period of 3 weeks, from 20.04.23 to 10.05.23, before the data collection was closed.

3.4 Reliability and Validity

According to Saunders (2015), the reliability of a questionnaire refers to its ability to be replicated and produce consistent results. To strengthen the reliability of this research, we aimed to minimize threats to reliability within the research methodology. To minimize participant error, we presented the estimated time frame for completion prior to the survey. This was done to avoid surprising respondents by the length of the survey, which could lead to a rush to complete. Further, we aimed to minimize participant bias, namely social desirability bias, by ensuring full anonymity of respondents to encourage truthful responses.

Validity refers to the appropriateness of the measure used in the survey, the accuracy of the analyses of results and the extent to which results are generalizable (Saunders, 2015, p. 202). The research method was consistent throughout the study and all participants received the same survey. The two variables, control and incentive, were introduced and measured in isolation to minimize confounding variables and improve internal validity. By aiming to include a broad sample across ages and nationalities, we intended to strengthen the external validity to make findings generalizable. To strengthen ecological validity, we used feasible real-life examples when introducing respondents to the different conditions and measurements in the survey.

In 4.0 Data Analysis we analyze the reliability and validity of the conceptual framework with the data collected for this research.

3.5 Compliance with Ethical and Legal Regulations

To comply with both Norwegian and BI regulations for data collection, respondents were first presented with a statement of informed consent regarding their participation, derived from Sikt (n.d.). The statement included the purpose of the study, and

information about how the data they provided would be processed. Respondents were ensured complete anonymity, as we did not ask for any information that could be identified or traced back to them, and IP address collection tools were turned off. To proceed with the survey, respondents had to state whether they agreed with this statement. Agreeing lead respondents through to the questionnaire, whereas disagreeing directed them to the end of the survey.

4.0 Data Analysis

In this chapter, we present the collected data and corresponding analyses. We have performed descriptive and statistical analyses for data exploration and to test hypotheses.

We received a total of 337 responses to the survey. We consider this sample size sufficient as we accept an error margin of 5.23%. The first step of data analysis consisted of cleaning the data in SPSS. After removing 135 responses, which were either incomplete or in progress, but not submitted when the survey was closed, we arrived at 202 complete responses.

4.1 Sample Demographics

In order to gain an understanding of the sample and the sample characteristics, we performed descriptive statistics, which are presented in Table 4.

Table 4. Descriptive Statistics of Sample

		Frequency	Percent
Gender	Male	68	33.66
	Female	132	65.35
	Prefer not to say	2	0.99
	Total	202	100.00
Age	18-24	48	23.76
	25-34	91	45.05
	35-44	12	5.94
	45-54	27	13.37
	55-64	20	9.90
	65+	4	1.98
	Total	202	100.00
Occupation	Student	23	11.39
	Student with a part-time position	47	23.27
	Part-time employee	12	5.94
	Full-time employee	107	52.97
	Self-employed	3	1.49
	Retired	3	1.49
	Other	7	3.47
	Total	202	100.00
Country	France	4	1.98
	Norway	187	92.57
	U.S.	4	1.98
	Other	7	3.47
	Total	202	100.00

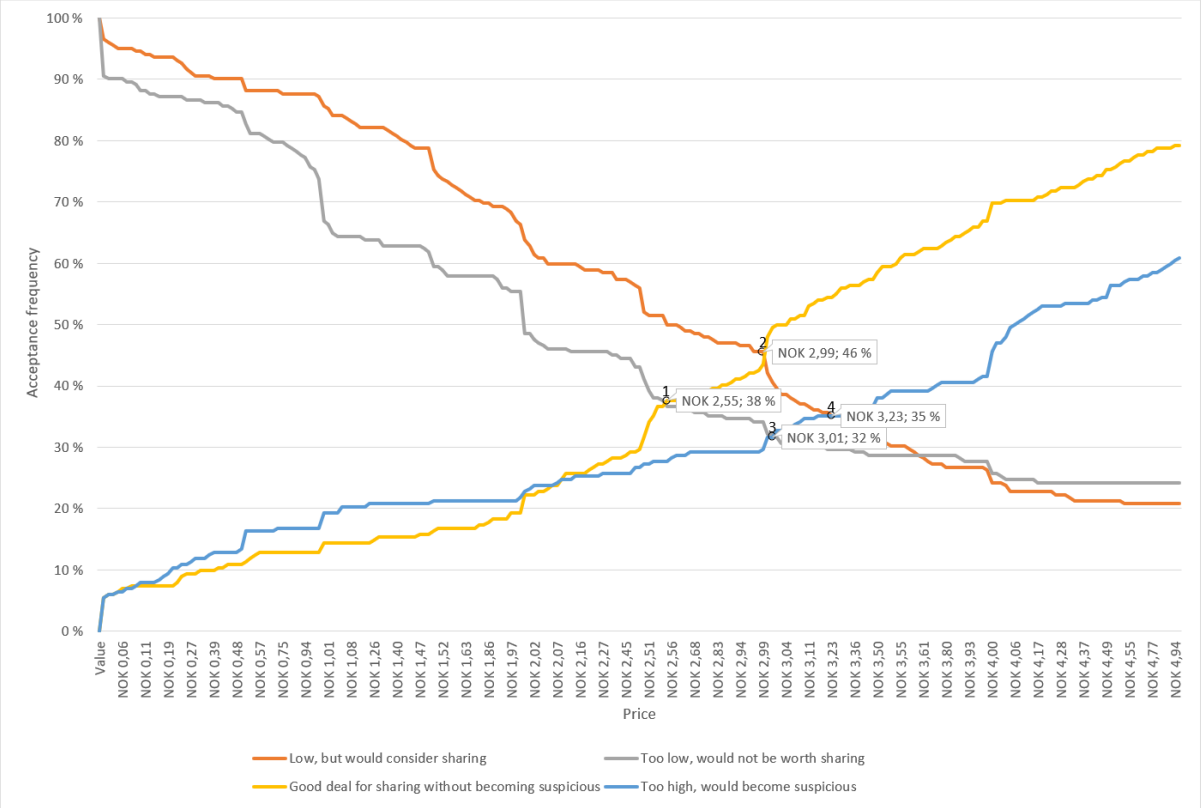
The final sample consisted of 68 males, 132 females, and 2 respondents who reported that they preferred not to state their gender. A large majority of the respondents, 92.6%, were residents in Norway, while 2% resided in France, 2% resided in the U.S., and the remaining 3.5% of respondents resided in other countries in Europe, North- and South America. The ages of the respondents ranged from 18 to 65 and over, with the majority of respondents (68.8%) being between 18 and 34 years old. As for occupation, half of the sample (53%) consisted of full-time employees, and 34.7% were students with or without a part-time job. The rest of the sample responded being part-time employees, retired, self-employed, or having other occupations.

4.2 Optimal Price Point for Data Exchange

We analyzed the data obtained from the questions asked using the Van Westendorp Price Sensitivity model to establish 4 price points for data exchange. To determine the different price points, we plotted the cumulative frequencies for each of the four questions against the price range on the same graph, as according to Ceylana et al.

(2014). The cumulative frequencies for “Low” and “Too Low” were inverted to ensure 4 intersecting points, as is the conventional practice for this approach (Chhabra, 2015, p. 262). Figure 2 shows the complete graph with the 4 price points.

Figure 2. Price Sensitivity Meter



Note: Point 1: Point of marginal cheapness, Point 2: Indifference price point, Point 3: Optimal Price point, Point 4: Point of marginal expensiveness

We find the range of acceptable price (between point 1 and point 4 in Figure 3) to be between NOK 2.55 and 3.23. The first price point (1) is the point where “Good deal for sharing without becoming suspicious” and “Too low, would not be worth sharing” intersect. This point is the lower bound of the acceptable price range and is often called the “point of marginal cheapness” (Chhabra, 2015, p. 262). In this study, we find this point to be at NOK 2.55. Similarly, price point 4, where “Low, but would consider sharing” and “Too high, would become suspicious” intersect, is regarded as the upper bound of the acceptable price range and is often referred to as the “point of marginal expensiveness” (Chhabra, 2015, 262). We find this point to be NOK 3.23. Between these two points, we find the range in which most consumers would find the price

acceptable (Van Westendorp, 1976, as cited in Chhabra, 2015). Within this range, we find price points 2 and 3. Price point 2 is where "Low, but would consider sharing" and "Good deal for sharing without becoming suspicious" intersect. This point is called the "indifference price point", where an equal number of respondents have rated the point as either of the two statements (Chhabra, 2015, p. 263). The indifference price point is at NOK 2.99. The last price point (3) is where "Too low, would not be worth sharing" and "Too high, would become suspicious" intersect, and is referred to as the "optimal price point" (Chhabra, 2015, p. 263). We find the optimal price point to be NOK 3.01. This suggests that the optimal price to offer a consumer for their data in the form of a micropayment is NOK 3.01 per data point exchanged. It would be interesting to study whether the optimal price point would differ across countries and nationalities. However, due to the small sample size of participants residing in another country than Norway, such analyses would not be meaningful with our data. Future research should consider studying this potential difference.

In the following section we evaluate the collected data on consumer awareness, attitude, and control, and the framework of digital personal data categories. To prepare the measures for hypothesis testing, we conducted factor analyses and evaluate the fit of the framework model.

4.3 Descriptive and Exploratory Analysis of Awareness, Attitude and Control

For a general overview of responses to the statements intended to measure awareness, attitude, and control in relation to online behavioral advertising, we performed descriptive statistics of the sample consisting of 202 respondents (for the statement "Suspicion" we have 1 missing value resulting in n = 201). For further use in hypothesis testing, we were also interested in exploring the relationships and underlying dimensions of the five statements. As the variable data is measured on a 5-point Likert scale, we used Spearman´s rank-order correlation method which is considered appropriate for measuring monotonic relationships with data measured at the ordinal level to create a correlation matrix (Hauke & Kossowski, 2011, p. 89). Results from the descriptive statistics and correlation matrix are presented in Table 5.

Table 5. Descriptive Statistics & Correlation Matrix

	n	Mean	SD	1	2	3	4
1. Awareness	202	2.82	1.30				
2. Understanding	202	3.54	1.14	.43***			
3. Control	202	3.74	1.08	.14**	.08		
4. Suspicion	201	3.56	1.15	.10	.10	.17**	
5. Usefulness	202	3.05	1.13	-.02	.12	.10	.34***

***Significant at the .01 level (two-tailed)
**Significant at the .05 level (two-tailed)

From mean ratings, we find that not being in control has the highest agreement score of 3.74 (SD = 1.08). Self-reported awareness is relatively high for both "Awareness" (M = 2.82, SD = 1.30) and "Understanding" (M = 3.54, SD = 1.14). Overall attitudes towards personalized advertisements are lower, but still relatively high, with a high agreement rating for "Suspicion" (M = 3.56, SD = 1.15), which decreases the overall attitude rating, and a high agreement rating for "Usefulness" (M = 3.05, SD = 1.13). For further analysis, the ratings for "Suspicion" and "Control" were reverse coded to ensure comparability and to measure an overall positive or negative attitude towards personalized advertisements among respondents.

From the correlation matrix (Table 5), we find that the first two statements, "Awareness" and "Understanding", intended to measure awareness, significantly correlate ($p < .001$). The two last statements, "Suspicion" and "Usefulness", intended to measure attitude, also significantly correlate ($p < .001$). Interestingly, we see that the statement measuring perceived control significantly correlates with "Awareness" ($p = .042$) and "Suspicion" ($p = .018$), suggesting a significant (positive) relationship between these statements. From the correlation matrix we found correlation loadings higher than .3, which suggests that exploratory factor analysis would be an appropriate analysis to run (Taherdoost et al., 2022, p. 377).

We further explored the underlying dimensions of the variables by performing a factor analysis. We first checked if the data was appropriate for a factor analysis by evaluating the Bartlett´s test of sphericity and the Keyser-Meyer-Olkin (KMO) measure of sampling adequacy. From the Bartlett´s test we got an approximate Chi-Square of 67.59 which is significant with a p-value < .001, suggesting appropriateness. The KMO measure gave a value of .496. High values for this test, suggesting that factor analysis is appropriate, are considered to be between 0.5 and 1.0 (Malhotra, 2020, p. 610). We recognize that the value is just below the lower bound of appropriateness at 0.5, but as it is very close to this value, we consider it acceptable. We initially ran the factor analysis with all five statements. As "control" did not load sufficiently high on either component, we excluded this statement and ran the analysis again. The resulting rotated component matrix with factor loadings is presented in Table 6.

Table 6. Rotated Component Matrix Awareness & Attitude

	Component	
	1	2
Awareness	.74	-.01
Understanding	.58	.13
Suspicion	.11	.47
Usefulness	-.02	.69

Extraction Method: Factor Analysis. Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 3 iterations.

From the results in Table 6, we find that the two statements intended to measure awareness ("Awareness" and "Understanding") do so, as they both load higher on component 1 (.74 and .58), while the two statements intended to measure attitude ("Suspicion" and "Usefulness") load higher on component 2 (.47 and .69).

4.4 Confirmatory Factor Analysis and Model Fit Evaluation of Framework

We performed a Spearman´s rank-order correlation analysis of the 17 items of digital personal data to evaluate patterns and associations within and between the categorization of the framework. The correlation matrix is presented in Appendix 4. Within the coefficient range of 0-1, we see tendencies of higher correlations between variables that are postulated to belong to the same categories, based on the theoretical basis of Chua et al. (2021), Gupta et al. (2010), Heirman et al. (2013), Milne et al.

(2017), Phelps et al. (2000), and Robinson (2017). We also see that variables for the most part do not correlate highly with variables of other categories, strengthening the divergent validity of the research. As correlation coefficients approximate to 1 indicate a positive relationship and approximate to 0 indicates a weak or no relationship, the pattern suggests that category specific items have stronger associations than those between categories (Saunders, 2015).

To evaluate the framework of 17 items measuring 6 categories of digital personal data, we performed a confirmatory factor analysis in AMOS. A confirmatory factor analysis is used to confirm whether certain variables correctly measure a certain factor and how well the collected data fit the hypothesized model (Janssens, 2008). The path diagram of digital personal data categories drawn for the confirmatory factor analysis is presented in Appendix 5. The resulting factor estimates are presented in Table 7.

Table 7. Factor Estimates & Significance

	Item	Estimate	Standardized Estimate	S.E.	C.R.	p-value
Socio-Demographic	3	**1.00**	.57			
	2	1.77	.77	.24	7.51	***
	1	1.64	.72	.23	7.27	***
Medical Health	1	**1.00**	.81			
	2	.98	.79	.14	6.79	***
Lifestyle-Behavior	3	**1.00**	.79			
	2	.98	.74	.09	10.49	***
	1	.88	.66	.09	9.28	***
	4	.91	.71	.09	10.01	***
Tracking	3	**1.00**	.77			
	2	1.07	.74	.13	8.51	***
	1	.58	.48	.10	6.00	***
Authenticating	3	**1.00**	.74			
	2	.33	.49	.05	6.26	***
	1	.56	.54	.08	6.97	***
Financial	1	**1.00**	.51			
	2	1.77	.57	.29	6.23	***

***p < .001

Note: Estimate: One item in each category fixed to 1.00

We evaluate the unidimensionality of the resultant model by considering the loadings of the items on the assigned categories and their significance. From the analysis, we see that all items load significantly, with *t*-values larger than 1.96 (Critical Ratio ≥ 6.00 for all variables). From the standardized estimate in table 7, we see that almost all items load sufficiently high (> .5), except Tracking 1 (.48) and Authenticating 2 (.49), which

loadings are just below the cut off-value, but close enough to be considered acceptable (Janssens, 2008).

We also consider the overall fit of the model based on measurements and indices presented in Table 8 and Table 9.

Table 8. Model Fit: Chi-Square

	CMIN	DF	p-value	CMIN/DF
Default model	349.98	104	.000***	3.37
Saturated model	.00			
Independence model	1468.24	136	.000***	10.80

***p < .001

Table 9. Goodness of Fit Index & Baseline Comparisons

	GFI	AGFI	TLI	CFI
Default model	.82	.73	.76	.82
Saturated model	1.00			1.00
Independence model	.36	.28	.00	.00

From interpretation of the results, the Chi-square (CMIN) of 349.98 (see Table 8) is significant (p = .000), which suggests that the covariance generated by the model is incongruent with the observed covariance (Marsh & Hocevar, 1985, p. 567). As the Chi-square almost always becomes statistically significant when the model contains many variables, this test alone is not sufficient to determine goodness of fit (Marsh & Hocevar, 1985, p. 567). Instead, we consider the ratio between the Chi-square and degrees of freedom. The ratio for the model is found to be within the acceptable range between 3 and 5 (CMIN/DF = 3.37) (see Table 8), indicating that the model is acceptable (Marsh & Hocevar, 1985, p. 567). Further, we can use the Goodness of Fit Index (GFI) to evaluate the fit of the model. The GFI of the model is .82 (see Table 9), making the fit somewhat less than reasonable as GFI > .9 is considered a reasonable fit (Janssens, 2008, p. 296). Lastly, we consider the Tucker-Lewis Index (TLI) and the Comparative Fit Index (CFI) which are considered some of the most reliable indices (Janssens, 2008, p. 296). These indices (see Table 9) suggest that the model has a less than optimal fit, as both are somewhat below the preferred value of .9 (TLI = .76, CFI = .82) (Janssens, 2008, p. 296).

We further evaluate the model by reliability and validity through composite reliability and average variance extracted presented in Table 10.

Table 10. Reliability & Validity Calculations

	Composite Reliability	Average Variance Extracted
1 Socio-Demographic	.73*	.48
2 Medical Health	.78*	.64*
3 Lifestyle-Behavior	.87*	.53*
4 Tracking	.71*	.45
5 Authenticating	.62*	.36
6 Financial	.45	.29
	*≥0.6	*≥0.5

Reliability is determined on a basis of the composite reliability of each item to its corresponding category, calculated by the formula below.

$$\textit{Composite reliability} = \frac{(\sum Standardized\ loadings)^2}{(\sum Standardized\ loadings)^2 + \sum measurement\ errors}$$

A composite reliability value higher than .6 is accepted as reliable (Fornell & Larcker, 1981). Calculations show that 5 out of 6 framework categories are reliable (Composite reliability > .6 for categories Socio-Demographic, Medical Health, Lifestyle-Behavior, Tracking, and Authenticating). The composite reliability for the remaining category Financial (CR = .45) is below the limit for verifying reliability. This result could be accounted for by a lack of shared variance among the Financial category items.

We further evaluate the framework by convergent validity (Janssens, 2008, p. 306). An initial assessment of convergent validity is the factor loadings and corresponding significance. All factor loadings should be higher than .5 and statistically significant (Malhotra, 2020, p. 702). The model satisfies these criteria for all but 2 items (Tracking 1 and Authenticating 2), which loadings are approximate to .5 and significant, as presented in Table 7. To further evaluate the validity of the framework, we calculated the average variance extracted to measure how much of the variance in the items may be explained by the categories. The average variance extracted was calculated for each category of the framework by the formula below, presented in Table 10. A value in the range of .5 or higher is considered acceptable (Malhotra, 2020, p. 702).

$$\textit{Average variance extracted} = \frac{\sum(standardized\ loadings)^2}{\sum(standardized\ loadings)^2 + \sum measurement\ errors}$$

The calculations in Table 10 show that only 2 categories, Medical Health and Lifestyle Behavior, meet the minimum criteria for average variance extracted of .5 to be considered acceptable. However, the categories Socio-Demographic (.48) and Tracking (.45) are close and approximate to acceptable values (Malhotra, 2020, p. 702). The remaining categories have values ranging below .50, indicating that less than 50% of the variance in the items is explained by the associated framework categories (Malhotra, 2020, p. 702). However, as the average variance extracted is considered a more conservative measure than composite reliability, we can conclude that the convergent validity is adequate as long as the composite reliability measure is above .6 (Fornell & Larcker, 1981, p. 46).

Based on the results from the confirmatory factor analysis, we see that the model has a subpar fit, although reliability and validity is adequate for 5 of the 6 categories. The suboptimal model fit is mainly due to the two variables, T1 and A2, which have somewhat lower loadings, and the category for Financial information, as this category includes two items which are rated differently in terms of willingness to share digital personal data. In reviewing the model, we need to decide to either remove variables and thereby improve the model or continue with the model as it is. Post hoc modifications to a model should only be made when there exists theoretical justification for it and the changes make sense (Harrington, 2009; Jackson et al., 2009). The framework for this model is previously tested and validated by previous research, and the items in question are important in order to holistically measure all aspects of digital personal data. Therefore, we do not remove any variables for further analysis, as they are important to include for the purpose of this research. However, we acknowledge that there are variations in the ratings of items within the proposed Financial category, resulting in low reliability, and that the category and its corresponding items should be further tested to conclude whether changes to this category or the framework should be made. This will be discussed further in 6.0 Implications and Limitations.

4.5 Consumer Willingness to Share Digital Personal Data

After evaluating the fit of the framework, we prepared the data on consumer willingness to share digital personal data for hypothesis testing. Respondents' mean category ratings were calculated by the corresponding items to create new variables representing willingness to share in each category of digital personal data. Repeating this procedure, we created a variable for overall willingness to share digital personal data, determined by the mean ratings across the 6 categories. Preparing the data for testing the hypothesized effects of control and incentives, we again repeated the procedure, creating new variables of the category specific items' mean ratings, and the overall mean ratings under these conditions.

To explore the collected data of respondents' willingness to share digital personal data in the baseline condition, we conducted descriptive statistics of the category variables. Table 11 displays the mean rank of consumers' willingness to share each category of digital personal data in the baseline condition. The means indicate that consumers are more willing to share data categorized as Socio-Demographic and Lifestyle-Behavior, and more apprehensive about sharing Authenticating and Tracking data. The lowest ranked means imply that consumers are least inclined to share data concerning Medical Health and Finance.

Table 11. Willingness to Share Categories of Digital Personal Data

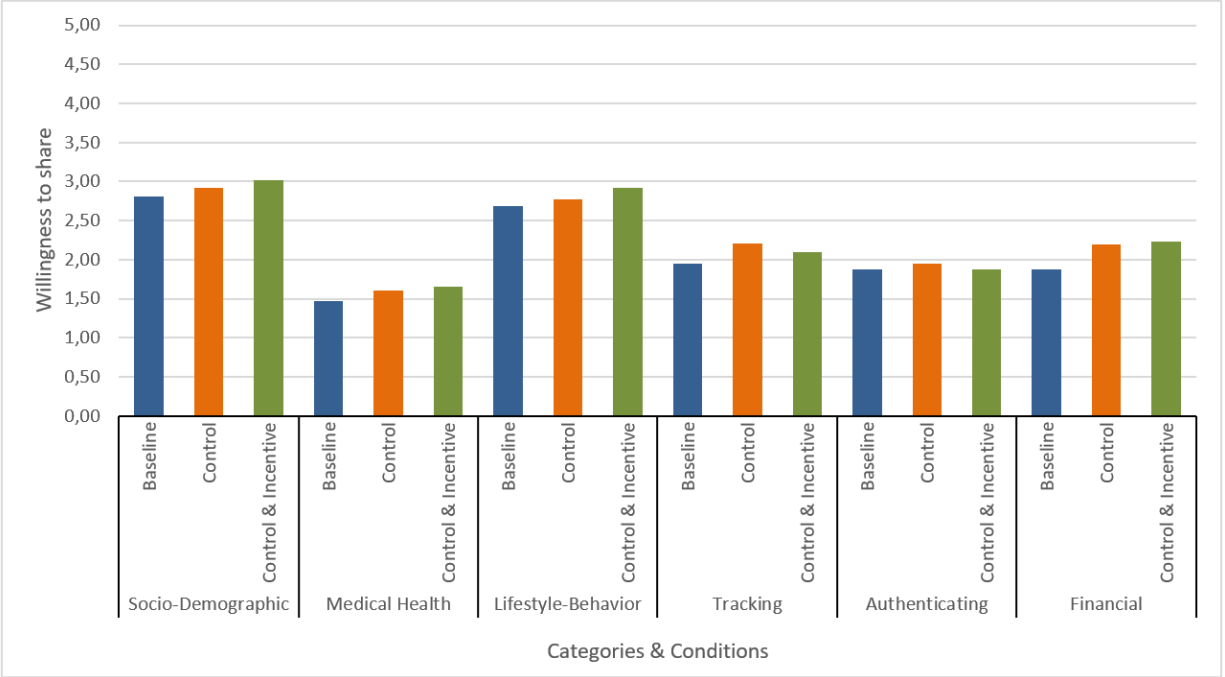
Category	Mean	Std. Deviation
Socio-Demographic	2.81	1.06
Lifestyle-Behavior	2.69	1.03
Tracking	1.95	.85
Authenticating	1.88	.80
Financial	1.87	.80
Medical Health	1.47	.80

We find no difference in willingness to share digital personal data between men (M = 2.10, SD = .74) and women (2.13, SD = .59) (p = .114). However, ANOVA analysis shows some significant differences in mean willingness to share between age groups. The age group 55-64 reported a significantly lower mean willingness to share (M = 1.66, SD = .63) than those belonging to the age groups 18-24 (M = 2.26, SD = .61, p = .005), 25-34 (M = 2.17, SD = .61, p = .017), and 35-44 (M = 2.37, SD = .90, p = .032). Analysis of willingness to share across employment status shows no significant differences in means between students (M = 2.33, SD = .63), students with a part-time

position (M = 2.32, SD = .58), part-time employees (M = 2.02, SD = .60, full-time employees (M = 2.02, SD = .66), self-employed (M = 1.93, SD = .77), retired (M = 1.74, SD = .76), and other employment status (M = 1.83, SD = .72), as all p-values are above 0.1.

We further analyzed consumers' ratings of willingness to share categories of digital personal data. Figure 3 displays the distribution of these rankings under the baseline condition, control condition, and the combined control and incentive condition.

Figure 3. Willingness to Share Data across Conditions & Categories



From Figure 3 we see that Socio-Demographic and Lifestyle-Behavior are the overall highest ranked categories across conditions, in contrast to Medical Health, which has the overall lowest ranked willingness.

4.6 Hypothesis Testing

4.6.1 Hypothesis 1

The first hypothesis, H1, predicts that there is a difference in willingness to share between the categories of digital personal data. A paired samples *t*-test was performed to pairwise test respondents' mean willingness to share across the 6 categories of digital

personal data. In order to include all possible combinations of the framework, a total of 15 category pairs were tested. The results are presented in Table 12.

Table 12. Pairwise t-tests: Digital Personal Data Categories

Category Pairs	Mean Difference	Std. Deviation	*t*-value	df	p-value
Socio-Demographic - Medical Health	1.34	1.05	18.11	201	<.001***
Socio-Demographic – Lifestyle-Behavior	.17	.84	1.98	201	.049**
Socio-Demographic – Tracking	.86	1.07	11.38	201	<.001***
Socio-Demographic – Authenticating	.93	1.06	12.50	201	<.001***
Socio-Demographic – Financial	.94	1.02	13.06	201	<.001***
Medical Health – Lifestyle-Behavior	-1.23	1.02	-17.10	201	<.001***
Medical Health – Tracking	-.49	.95	-7.29	201	<.001***
Medical Heath - Authenticating	-.41	.95	-6.18	201	<.001***
Medical Health – Financial	-.41	.970	-5.95	201	<.001***
Lifestyle-Behavior – Tracking	.74	.99	10.60	201	<.001***
Lifestyle-Behavior – Authenticating	.81	.99	11.66	201	<.001***
Lifestyle-Behavior – Financial	.82	.94	12.41	201	<.001***
Tracking – Authenticating	.07	.79	1.34	201	.182
Tracking – Financial	.08	.87	1.32	201	.190
Authenticating - Financial	.01	.72	0.13	201	.896

*** p<.001 ** p<0.05 *p<.1

From table 12, we find statistically significant differences in mean willingness to share at a 5% significance level for 12 pairs. We do not find a significant difference in means for the remaining 3 category pairs, namely Tracking-Authenticating ($t(201) = 1.34$, $p = .182$), Tracking-Financial ($t(201) = 1.32$, $p = .190$) and Authenticating-Financial ($t(201) = .13$, $p = .896$). This suggests that there is a difference in consumers' willingness to share digital personal data depending on the category of data, with a few exceptions. Thus, we find partial support for H1.

4.6.2 Hypothesis 2

The second hypothesis, H2, predicts that awareness of online behavioral advertising and attitude towards personalized advertisements will positively affect consumer willingness to share digital personal data. To test the effect of the independent variables Awareness and Attitude on the dependent variable Willingness to Share digital personal data, we performed a linear regression analysis. Descriptive statistics for the three variables are presented in Table 13, and regression coefficients are presented in Table 14.

Table 13. Descriptive Statistics of Independent & Dependent Variables

	Mean	Std. Deviation
Willingness to Share	2.11	.65
Awareness	3.17	1.03
Attitude	2.75	.93

Table 14. Regression Coefficients: Awareness & Attitude on Willingness to Share

	Unstandardized B	Coefficients Std. Error	Standardized Coefficients Beta	*t*-value	p-value
Constant	1.55	.18		8.57	<.001***
Awareness	-.05	.04	-.08	-.1.28	.202
Attitude	.27	.05	.38	5.80	<.001***

R^2 .147
Adjusted R^2 .139

From the regression analysis, we see a slight negative tendency, but find no statistical support for a linear relationship between awareness of online behavioral advertising and consumer willingness to share digital personal data (β = -.05, p = .202). We do, however, find statistical support for a linear relationship between attitude towards personalized advertisements and consumer willingness to share digital personal data at the 1% level (β = .27, p < .001). The positive relationship suggests that if attitude ratings increase by 1 point, willingness to share will increase by 27%. The adjusted R^2 of .139 shows that the model explains 13.9% of the variation within the willingness to share variable. This is a very interesting finding as attitude towards personalized advertisements resultantly explains a considerable amount of the variance within willingness to share digital personal data. The linear regression analysis shows partial support for H2.

4.6.3 Hypothesis 3

Hypothesis 3 predicts that being in control of digital personal data will positively affect consumers' willingness to share across all categories of digital personal data. To test this hypothesis, we conducted a paired samples *t*-test for each of the category means under the control condition versus the baseline rating. Results from the pairwise *t*-tests are presented in Table 15.

Table 15. Pairwise t-tests: Willingness to Share Baseline and Control Condition

Baseline	Control Condition	Mean Difference	Std. Deviation	*t*-value	df	p-value
Socio-Demographic	Socio-Demographic	.11	.88	1.81	201	.036**
Medical Health	Medical Health	.14	.70	2.79	201	.003**
Lifestyle-Behavior	Lifestyle-Behavior	.08	.81	1.35	201	.089*
Tracking	Tracking	.25	.88	4.07	201	<.001***
Authenticating	Authenticating	.07	.61	1.58	201	.058*
Financial	Financial	.33	.88	5.31	201	<.001***

*** p<.001 ** p<0.05 *p<.1

We find that all categories have a positive mean difference, meaning willingness to share increases to some degree in all categories of digital personal data under the control condition. The category in which willingness to share increases the most is Financial (MD = .33, SD = .88), with Tracking being the second most increasing category (MD = .25, SD = .88). We also find a relatively high increase in Medical Health (MD = .14, SD = .70), followed by Socio-Demographic (MD = .11, SD = .88). Lastly, we see the least increase in Lifestyle-Behavior (MD = .08, SD = .81) and Authenticating (MD = .07, SD = .61). The increases in mean ratings of consumers' willingness to share digital personal data under the control condition are statistically significant across 4 categories at the 5% level, and all categories at the 10% level. Thus, we find support for H3.

4.6.4 Hypothesis 4

To test Hypothesis 4, in which we predict a positive effect of monetary incentives on consumer willingness to share digital personal data across all categories, we again ran a paired samples *t*-test on category means, comparing the marginal difference in mean ratings between the control condition and the incentive condition. Results from the pairwise *t*-tests are presented in Table 16.

Table 16. Pairwise t-tests: Willingness to Share Control and Incentive Condition

Control Condition	Incentive Condition	Mean Difference	Std. Deviation	*t*-value	df	p-value
Socio-Demographic	Socio-Demographic	.10	1.03	1.42	201	.079*
Medical Health	Medical Health	.06	.82	.95	201	.173
Lifestyle-Behavior	Lifestyle-Behavior	.15	.87	2.48	201	.007**
Tracking	Tracking	-.11	.83	-1.93	201	.028
Authenticating	Authenticating	-.07	.63	-1.57	201	.059
Financial	Financial	.03	.77	.50	201	.307

*** p<.001 ** p<.05 *p<.1

From the results of the *t*-tests, we find that the mean difference in ratings for 4 of the 6 categories increase as we introduce the possibility of receiving payments for sharing digital personal data. We find support for the hypothesized effect at the 5% significance level only for the Lifestyle-Behavior category (MD = .15, SD = .87). At the 10% significance level we also find a significant increase in mean ratings under the incentive condition for the Socio-Demographic category (MD = .10, SD = 1.03).

Interestingly, we find tendencies of a reversed effect of incentives for the categories Tracking and Authenticating, as the mean ratings decrease when we introduce the scenario of receiving a monetary payment for sharing data. We see the largest decrease in the category Tracking with a mean difference of -.11 (SD = .83), while the category Authenticating has a mean difference of -.070 (SD = .63).

The findings suggest that providing consumers with monetary incentives for their digital personal data increases willingness to share only for the data they are already inclined to share. Considering we only find a statistically significant increase in willingness to share for 2 of the 6 categories, H4 is rejected.

4.7 Summary of Results

In Table 17 we present an overview of the hypotheses and the outcomes of the corresponding hypothesis tests.

Table 17. Summary of Hypothesis Outcomes

Hypothesis	Hypothesized Effect	Outcome
H_1: *Consumers' willingness to share personal data for marketing purposes differ between categories of digital personal data*	N/A	Partially Supported
H_2: *Consumer awareness of and attitude toward online behavioral advertising has a positive effect on consumers' willingness to share digital personal data with companies for marketing purposes*	+	Partially Supported
H_3: *Having control over own data positively affects consumers´ willingness to share all categories of digital personal data for marketing purposes*	+	Supported
H_4: *Monetary incentives positively affect consumers´ willingness to share all categories of digital personal data for marketing purposes.*	+	Rejected

5.0 Discussion

The aim of this study is to investigate implications of a potential blockchain-based system where consumers control and are incentivized for the exchange of their data. Based on previous literature on related topics, we formulated 4 hypotheses which have guided the data collection and analyses to explore the following research questions:

How is consumer willingness to share digital personal data impacted by attitude and awareness towards online behavioral advertising, and affected when offered the ability to control their own data, incentivized by micropayments, in a marketing setting? What is the optimal micropayment to receive in exchange for digital personal data?

The contributions of this research are insights in consumers´ willingness to share digital personal data in general, as well as under control and incentive conditions, and the effects of awareness and attitude towards online behavioral advertisements. Finally, we provide an optimal price to facilitate data exchange from a consumer perspective. Understanding what drives consumer willingness to share data is beneficial for marketers to gain an initial insight into the effects that a potential blockchain based data exchange system can entail. In this section we will discuss the research findings more in depth.

One of the main contributions of this study is the discovered price range of acceptable micropayments and the optimal price for consumers to receive in exchange for their digital personal data, which we found to be NOK 3.01 (approximately USD 0.30). The acceptable price range was found to be between NOK 2.55 and NOK 3.23. As previous studies on valuation of consumers´ digital personal data have mainly concerned payments of larger values, this study is one of the first to suggest an optimal price point for micropayments (Carrascal et al., 2013; Gabisch & Milne, 2014; Weydert et al., 2020).

Similar to findings of previous research, but opposed to findings of Chua et al. (2021), we found no significant difference in consumer willingness to share digital personal data between genders (Heirman et al., 2013; Robinson, 2017, p. 575). This result could be explained by the skewness of gender distribution in our sample. However, together with previous research, we see a theoretical weightage leaning towards excluding gender as an impacting factor on consumers' willingness to share data. Similarly to findings of Chua et al. (2021), analysis showed that consumers aged 55 and over, were generally less willing to share data, with the age group 55-64 being the least willing to share. Building on the validated frameworks of previous research, we add to the research on consumers' willingness to share digital personal data by updating items for recent technological developments and broadening the demographic reach of the framework.

Congruent with the findings of Weydert et al. (2020), we found a generally low baseline mean rating of willingness to share digital personal data across all categories. We also found that consumers´ willingness to share digital personal data differs depending on the type of data requested, with a few exceptions, partly supporting H1. Moreover, we found that consumers are most willing to share digital personal data belonging to the categories Socio-Demographic and Lifestyle-Behavior, in line with Chua et al. (2021), who found these two categories to be rated lowest on privacy concern and highest on disclosure intention. This finding might be explained by the general risk related to disclosing these types of information and their relevance in a marketing context. As explained by Culnan & Bies (2003), the risk associated with sharing personal information needs to be exceeded by the perceived benefit of sharing that information.

The higher willingness to share Socio-Demographic and Lifestyle-Behavior information suggests that consumers perceive the risk associated with sharing this information to be lower than the perceived benefit of sharing. As relevance is found to decrease risk perceptions and increase attitudes towards information sharing, both category of information and the context in which it is requested is suggested to be of importance (Zimmer et al., 2010). In a marketing context, several of the items within the two highest ranked categories, such as demographics, physical characteristics, interests, and media behavior, can by the consumer intuitively be regarded as relevant information to collect. Tracking, the third highest ranked category, can also be regarded as relevant information in a marketing context for someone with knowledge and understanding about online behavioral advertising. However, this type of information seems to be considered more sensitive. The three lowest ranked categories, Authenticating, Financial, and Medical Health, were found by Chua et al. (2021) to carry a higher privacy concern. The risk of sharing these types of data might therefore be perceived as higher than the potential benefit, and the relevance to the marketing context might not be perceived as clear.

An interesting finding is that for the current study, consumers reported they were least willing to provide digital personal data on their Medical Health, whereas the same category was ranked number 3 out of 6 in the study by Chua et al. (2021, p.11). This might be due to cultural differences between the samples, as the forementioned research studied Malaysians, whereas our sample almost exclusively consisted of Norwegians. Confirming the results of Chua et al. (2021), the categories Finance and Authenticating were not found to have significantly different ratings. The homogeneity in mean ratings suggests that it could be beneficial to combine these categories in the framework of digital personal data, however more research is needed.

In line with findings by Dehling et al. (2019) and Li & Nill (2020), we predicted that consumers with high awareness of how data is collected and used for targeting and advertising would be more willing to share their data, as highly aware consumers have been found to be less concerned about online behavioral advertising (Dehling et al., 2019). We did not find evidence of this. However, we found evidence which suggests that attitude towards personalized advertisements positively affects consumers'

willingness to share digital personal data, partially supporting H2. This finding postulate that consumer awareness of data collection and online behavioral advertising is not sufficient to predict their willingness to share digital personal data. It is the consumers' attitude towards online behavioral advertising which can in part predict their willingness to share. This is an interesting finding, as it adds to the literature on variables which can explain willingness to share data.

We also found a correlation between perceived control and attitude towards online behavioral advertisements, through the statement about suspicion. This finding is consistent with Baek & Morimoto (2012), stating that experiencing a lack of choice and control can lead to resistance towards personalized advertising. Reversely, this finding suggests that a strong sense of control correlates with a more positive attitude towards personalized ads, which can result in higher willingness to share digital personal data. This further validates the findings supporting H3, which predicted that control would increase consumer willingness to share digital personal data. Additionally, findings suggest that there is a relatively low perception of control over own data among internet users today. The relationship between control and attitude adds to the explanation of the personalization paradox. Aguirre et al. (2015) found that consent and transparency in the data collection process explains the difference in consumer response rates when they exposed to highly personalized ads. We add to the explanation of the personalization paradox, by suggesting that the degree to which a consumer perceives they are in control over the collection and use of their digital personal data influences their attitude towards receiving personalized advertisements.

Analysis results indicate that both control and monetary incentives increase consumer willingness to share digital personal data to some degree. Being in control over own data was found to significantly increase willingness to share all categories of digital personal data for marketing purposes, supporting H3. This is an important contribution to the limited theory on the effects of control on consumer willingness to share digital personal data. Contrary to our expectations, monetary incentives did not increase willingness to share in all categories, as we found tendencies of negative effects in two of the categories, Tracking and Authenticating. For these two categories, mean ratings

of willingness to share digital personal data decreased as respondents were offered monetary incentives.

The finding that monetary incentives did not significantly increase all categories of willingness to share, and the corresponding rejection of hypothesis H4, is not in line with findings of previously presented literature. This could, in part, be due to the lack of accounting for consumer control in previous research on consumer willingness to share digital personal data in exchange for benefits, as this is identified as the main driver of the increase in willingness to share in this study. The finding also contradicts the findings of Weydert et al. (2020). While they found that monetary incentives had a slightly negative effect on consumers' willingness to share data when the sensitivity of the data was perceived as low, we find a negative effect on willingness to share data types considered to be associated with high privacy concern, according to Chua et al. (2021). As Weydert et al. (2020) explains, the monetary incentive offered can signal a potential privacy protection loss and thereby reduce consumer willingness to share digital personal data. It is worth noting that in the study by Weydert et al. (2020) participants were offered a high amount of money in exchange for data, whereas in this study, we offered micropayments in the form of very low amounts of money. Our results, in line with the reasoning of Weydert et al. (2020), suggest that monetary incentives can raise suspicion, reversing the effects of control and making consumers less inclined to share data. Monetary incentives seem to increase the perceived risk associated with sharing high sensitivity categories of information to a level where the benefits of sharing data, such as money and personalized advertisements, are not perceived to be greater than the risk of sharing data. Further research should look into whether this finding is consistent, and the incentive level threshold for which this effect appears.

6.0 Implications and Limitations

6.1 Managerial Implications

The findings of this study have important implications for marketers and managers as they will, in the years to come, rely on consumers to willingly provide their personal information (Hemker et al., 2021, p.). Firstly, rather than relying on privacy policies to

mitigate consumer perceived risk, which can induce the bulletproof glass effect, consumer control over own data can encourage consumers to share any type of digital personal data. Giving consumers full access to the information collected about them and how this information is used, as well as the option to withdraw access to information, can increase their willingness to share their digital personal data for marketing purposes. Based on previous literature and our findings, we also suggest that offering consumers control over their information can increase their attitudes towards personalized advertisements utilizing this information, and reduce the negative effects explained by the personalization paradox further enhancing advertising response.

Applying the Van Westendorp model, we found in our study an acceptable price range between NOK 2.55 and 3.23, with an optimal price point of NOK 3.01 for sharing digital personal data. To our knowledge, our study is the first to suggest a specific amount of micropayment to offer consumers in exchange for their data. We also suggest that offering a higher amount than NOK 3.23 can be unwise, as this is found to be the threshold for which suspicion towards the intended use of the collected data is among consumers. On the other end, offering an amount lower than NOK 2.55 might not be sufficient to incentivize consumers to share their personal data. As previously mentioned, we also found evidence suggesting that monetary incentives are only efficient to increase consumers' willingness to share digital personal data related to the two categories Socio-Demographic and Lifestyle-Behavior, which should be taken into account if an implementation of this system is being considered.

The initial analysis of demographics showed a significant difference in consumers' willingness to share digital personal data in terms of age group. Older aged consumers, specifically those belonging to the group 55-64, are less willing to share all categories of digital personal data, which holds implications for both current and potential data collection practices. This finding suggests a generational divide between segments which can impact the effectiveness of data collection and targeting efforts. If this finding is generalizable for populations, managers must facilitate data collection methods to meet age specific segments' needs, in order to effectively collect data. Further research is needed to explore demographic specific drivers and barriers of

willingness to share, to identify underlying structures of data collection. This will be discussed further under 7.0 Further Research.

6.2 Limitations

As with any study, there are limitations to consider regarding this research. The first of which is in relation to the sample size, which might have impacted the generalizability of the data. In a research context, the final sample of 202 respondents is relatively small, which results in low variability between gender, age groups and occupation. As this study is relevant for anyone using the internet, we aimed for a large and geographically representative sample to make the findings generalizable. We were not able to include as many international respondents as we had hoped, thereby limiting the generalizability of the findings. To overcome this limitation, it could be necessary to repeat this study with a larger sample.

Reliability and validity measures provided satisfactory results in 5 of the 6 framework categories, as the category Financial did not meet the criteria for sufficient scores. Although this result somewhat limits the validity and generalizability of this research, we concluded that it was purposeful to keep the framework composition of 6 categories and 17 items. The reasoning for this being that the framework consists of all aspects of digital personal data, and removing a category would limit the holistic measure of consumers' willingness to share digital personal data. Further, there was no theoretical ground for altering the framework for this study as it has been validated in previous research, most recently by Chua et al. (2021), which can somewhat increase the confidence of our findings (Christensen et al., 2022).

From the open text response field, we received some responses regarding the Van Westendorp Price Sensitivity Meter. A few were concerned about the forced response of questions, meaning they had to set a value within the monetary scale to proceed with the survey. We found it necessary to force answers within a set scale to these questions, to perform analyses and identify optimal price points. These concerns do, however, voice a limitation to the study as those who did not want to answer, or did not have an answer that fit within that range, had to select price points. We saw tendencies in the data set for responses maximized to 5, as well as minimized to 0 for all questions, which

limits the validity of the data and analysis of the Van Westendorp Price Sensitivity Meter. However, the data gave meaningful results for a price sensitivity analysis, as the mean selected price for each question ranged increasingly within the set price range.

It is worth noting that the statements asked to measure awareness do not reflect how aware each respondent truly is. In retrospect, we acknowledge that asking respondents to answer knowledge questions about data collection and use, would perhaps reflect actual awareness better, rather than self-perceived awareness. This adjustment could have better supported the persuasion knowledge model, which might have yielded different results. Similarly, we have identified a limitation regarding the framework. When applying the framework, mainly adopted from the studies of Chua et al. (2021), we included 17 items instead of the 22 items of their research, to avoid fatigue and dropout by respondents, as they were asked to rate their willingness to share these items three times under different conditions. As we still tried to include and capture the content of most items, we truncated and combined some items and worded some items differently than previous research. This could potentially be a contributing factor to the subpar model fit from the Confirmatory Factor Analysis, and corresponding reliability and validity tests, particularly for the category Financial.

There are also some limitations regarding the presentation of the control and incentive conditions in our survey that are worth acknowledging. One of these limitations, are the examples used to test willingness to share. The differences in findings under the control condition and the incentive condition could potentially stem from differences in the two presented examples. It would be interesting to see if we would get the same results if we used the exact same example in the two conditions. Another limitation is that willingness to share in the baseline, but also in the control and incentive condition, might be highly dependent on the type of company that is requesting the information and where the company operates. As one respondent wrote as a comment for the survey: “Depending on what country the company is registered in, it might change my attitude and willingness to share”. For the scope of this research, we wanted to explore a general willingness to share under the different conditions and did not include any specific types of companies or company names to purposely avoid influencing the

ratings. However, we do acknowledge that willingness to share digital personal data may differ given which company is requesting the information.

Several studies suggest the existence of a discrepancy between how concerned people say they are about their data and privacy online, and how they behave online (Brown, 2001; Norberg et al., 2007). This discrepancy is known as the privacy paradox (Norberg et al., 2007). With the data collection method used for this research, where we ask participants to state what they think, rather than observe what they actually do, we might find this paradox to influence results. Asking participants to state their willingness to share different types of digital personal data might have activated a privacy concern that would not have been activated had they been in a more organic setting. This potential limitation can be overcome by replicating the research in a physical experiment setting.

7.0 Further Research

Due to the limited sample size, we recommend further research to repeat the study on larger samples and different cultures, as well as perform practical experiments to expand on the findings and improve generalizability. Conducting replicative and larger studies to validate the framework employed in this study could further reduce the associated limitations discussed above.

Consistent with the findings of this study, literature on consumers' willingness to share digital personal data in different cultures, has provided similar rank orders of willingness to share categories of personal data (Chua et al., 2021; Gupta et al., 2010; Milne et al., 2017; Phelps et al., 2000). Further research on the field could explore underlying factors and tendencies that explain this rank order, as could be the level of privacy associated with the categories that tend to cluster on a higher or lower rank. Additionally, it would be interesting to study whether the finding of low willingness to share Medical Health information is due to the sample size, the culture studied, or a possible change in consumers' privacy associated with their Medical Health data.

Building on our findings about willingness to share digital personal data with companies, further research should look into the effect that the location and type of

company has on willingness to share data in all three conditions. As the findings about receiving monetary incentives for sharing are not conclusive across studies, it would be interesting to study whether the company that requests this information influences willingness to share digital personal data in a marketing setting. We also urge further research to expand on the finding of monetary incentives having low, no, or reversed effect on consumer willingness to share, depending on the category of digital personal data. Qualitative and more in-depth research on drivers of consumer risk-perception and suspicion towards incentivizing data, could uncover underlying variables, and further explain the variation in the effect of monetary incentives. Such research will also be relevant for implementation of blockchain technologies in various industries, with its potential capabilities to perform micropayments.

Further research on micropayments and blockchain facilitated systems is needed to further explore price ranges exceeding the frame set for this research of NOK 0-5. It would be interesting to replicate this research with wider ranges, to rule out a potential central tendency bias, if the optimal price of NOK 3.01 remains constant. As we found monetary incentives to have an inconsistent effect on willingness to share across categories, replicating this study's modified Price Sensitivity Meter on the individual categories of digital personal data could uncover variations in optimal price points. Such research can provide a deeper understanding of how incentives can impact consumers' willingness to share digital personal data.

8.0 Conclusion

The purpose of this study was to add to the literature on consumer willingness to share digital personal data, exploring the potential effects of a blockchain based data sharing system where consumers control, and are incentivized for, their own data.

In conclusion, the study found that the general consumer willingness to share digital personal data is low, and that the willingness to share is to some extent dependent on the category of digital personal data. The study suggests that consumers´ attitudes towards personalized advertisements can positively affect their willingness to share information. When given the ability to control their own data, this study also suggests that consumers will be more willing to share all categories of digital personal data.

Monetary incentives in the form of micropayments were found to further increase consumers' willingness to share in only two categories of digital personal data, namely Socio-Demographic and Lifestyle-Behavior. This research also suggests a provisionally acceptable price range for data, where consumers evaluate NOK 3.01 as an optimal micropayment for their digital personal data. In a marketing setting, these findings imply that a potential blockchain facilitated system in which consumers receive control over, and potentially incentives for, their own data is a possible replacement for the current "cookies". This system would directly and securely transfer digital personal data between consumers and companies, which could be beneficial for both consumers and marketers.

References

Ackermann, K. A., Burkhalter, L., Mildenberger, T., Frey, M., & Bearth, A. (2022). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. *Journal of Consumer Behaviour*, *21*(2), 375–386. https://doi.org/10.1002/cb.2012

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, *91*(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005

Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). Data-driven digital advertising: Benefits and risks of online behavioral advertising. *International Journal of Retail & Distribution Management*, *49*(7), 1089–1110. https://doi.org/10.1108/IJRDM-10-2020-0410

Baek, T. H., & Morimoto, M. (2012). Stay Away From Me. *Journal of Advertising*, *41*(1), 59–76. https://doi.org/10.2753/JOA0091-3367410105

Benndorf, V., & Normann, H.-T. (2018). The Willingness to Sell Personal Data. *The Scandinavian Journal of Economics*, *120*(4), 1260–1278. https://doi.org/10.1111/sjoe.12247

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, *7*, 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872

Brough, A., Norton, D., & John, L. (2019). The Bulletproof Glass Effect: The Ironic Impact of Privacy Policies on Perceived Security and Purchase Intent. In *Advances in Consumer Research* (Vol. 47, pp. 40–44). Association for Consumer Research. https://www.acrwebsite.org/volumes/2551373/volumes/v47/NA-47

Brown, B. (2001). *Studying the internet experience* (HPL-2001-49). https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf

Bump, P. (2022, July 27). The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2023 Phase-Out. *HubSpot*. https://blog.hubspot.com/marketing/third-party-cookie-phase-out

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & De Oliveira, R. (2013). Your browsing behavior for a big mac: Economics of personal information online. In *WWW '13: Proceedings of the 22nd international conference on World Wide Web* (pp. 189–200). Association for Computing Machinery. https://dl.acm.org/doi/10.1145/2488388.2488406

Celsi, R. L., & Olson, J. C. (1988). The Role of Involvement in Attention and Comprehension Processes. *Journal of Consumer Research, 15*(2), 210–224. https://www.jstor.org/stable/2489526

Ceylana, H. H., Koseb, B., & Aydin, M. (2014). Value based Pricing: A Research on Service Sector Using Van Westendorp Price Sensitivity Scale. *Procedia - Social and Behavioral Sciences*, *148*, 1–6. https://doi.org/10.1016/j.sbspro.2014.07.013

Chhabra, S. (2015). Determining the Optimal Price Point: Using Van Westendorp's Price Sensitivity Meter. In S. Chatterjee, N. P. Singh, D. P. Goyal, & N. Gupta (Eds.), *Managing in Recovering Markets* (pp. 257–270). Springer India. https://doi.org/10.1007/978-81-322-1979-8

Chowdhury, M., Colman, A., Kabir, A., Han, J., & Sarda, P. (2018, August 1). *Blockchain as a Notarization Service for Data Sharing with Personal Data Store*. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, New York, USA. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00183

Christensen, R., Hodges, C. B., & Spector, J. M. (2022). A Framework for Classifying Replication Studies in Educational Technologies Research. *Technology, Knowledge and Learning*, *27*(4), 1021–1038. https://doi.org/10.1007/s10758-021-09532-3

Chua, H. N., Ooi, J. S., & Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security*, *110*(102453), 1–21. https://doi.org/10.1016/j.cose.2021.102453

Columbus, L. (2014, January 12). *2014: The Year Big Data Adoption Goes Mainstream In The Enterprise*. Forbes. https://www.forbes.com/sites/louiscolumbus/2014/01/12/2014-the-year-big-data-adoption-goes-mainstream-in-the-enterprise/

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, *59*(2), 323–342. https://doi.org/10.1111/1540-4560.00067

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2015). Is this for me? How Consumers Respond to Personalized Advertising on Social Network Sites. *Journal of Interactive Advertising*, *15*(2), 124–134. https://doi.org/10.1080/15252019.2015.1082450

Dehling, T., Zhang, Y., & Sunyaev, A. (2019). Consumer Perceptions of Online Behavioral Advertising. *2019 IEEE 21st Conference on Business Informatics (CBI)*, *01*, 345–354. https://doi.org/10.1109/CBI.2019.00046

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45–58. https://doi.org/10.1016/j.jnca.2018.10.020

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

Friestad, M., & Wright, P. (1994). The Persuasion Knowledge Model: How People Cope with Persuasion Attempts. *Journal of Consumer Research*, *21*(1), 1–31. https://www.jstor.org/stable/20798403

Gabisch, J. A., & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing*, *31*(1), 13–26. https://doi.org/10.1108/JCM-10-2013-0737

Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). FACILITATING GLOBAL E-COMMERCE: A COMPARISON OF CONSUMERS' WILLINGNESS TO DISCLOSE PERSONAL INFORMATION ONLINE IN THE U. *Journal of Electronic Commerce Research*, *11*(1).

Harrington, D. (2009). *Confirmatory Factor Analysis*. Oxford University Press, USA.

Harvey, C. R., Moorman, C., & Castillo Toledo, M. (2018). How Blockchain Will Change Marketing As We Know It. *SSRN Electronic Journal*, 1–6. https://doi.org/10.2139/ssrn.3257511

Hauke, J., & Kossowski, T. (2011). Comparison of Values of Pearson's and Spearman's Correlation Coefficients on the Same Sets of Data. *QUAGEO*, *30*(2), 87–93. https://doi.org/10.2478/v10117-011-0021-1

Heirman, W., Walrave, M., Ponnet, K., & Gool, E. V. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *7*(3). https://doi.org/10.5817/CP2013-3-3

Hemker, S., Herrando, C., & Constantinides, E. (2021). The Transformation of Data Marketing: How an Ethical Lens on Consumer Data Collection Shapes the Future of Marketing. *Sustainability*, *13*(20), 1–13. https://doi.org/10.3390/su132011208

Herzberg, A. (2003). Micropayments. In W. Kou (Ed.), *Payment Technologies for E-commerce* (pp. 245–282). Springer-Verlag. https://doi.org/10.1007/978-3-662-05322-5_12

Hughes, J., Camden, A., & Yangchen, T. (2016). Rethinking and Updating Demographic Questions: Guidance to Improve Descriptions of Research Samples. *Psi Chi Journal of Psychological Research*, *21*, 138–151. https://doi.org/10.24839/2164-8204.JN21.3.138

Jackson, D. L., Gillaspy, J. A., & Purc-Stephenson, R. (2009). Reporting practices in confirmatory factor analysis: An overview and some recommendations. *Psychological Methods*, *14*(1), 6–23. https://doi.org/10.1037/a0014694

Janssens, W. (2008). *Marketing Research with SPSS*. Prentice Hall/Financial Times.

Kiyomoto, S., Tanaka, T., Nakao, K., & Yamada, A. (2004). Implementation and Evaluation of a Micropayment System for Mobile Environments. *IPSJ Journal*, *45*(3), 870–879.

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Transactions on the Web*, *15*(4), 1–42. https://doi.org/10.1145/3466722

Kuhn, D. R. (2022). *A Data Structure for Integrity Protection with Erasure Capability* (NIST CSWP 25). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.25.pdf

Laurence, T. (2019). *Blockchain for dummies* (2nd ed.). John Wiley & Sons, Inc.

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., & Cranor, L. F. (2013). What matters to users?: Factors that affect users' willingness to share information with online advertisers. *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 1–12. https://doi.org/10.1145/2501604.2501611

Li, H., & Nill, A. (2020). Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy? *Journal of Consumer Policy*, *43*(4), 723–745. https://doi.org/10.1007/s10603-020-09469-7

Lipovetsky, S. (2006). Van Westendrop Price Sensitivity in Statistical Modeling. *International Journal of Operations and Quantitative Management*, *12*(2), 141–156.

Lundqvist, T., de Blanche, A., & Andersson, H. R. H. (2017). Thing-to-thing electricity micro payments using blockchain technology. *2017 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS.2017.8016254

Malhotra, N. K. (2020). *Marketing Research: An Applied Orientation* (7th ed.). Pearson.

Marsh, H. W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First- and higher order factor models and their invariance across groups. *Psychological Bulletin*, *97*(3), 562–582. https://doi.org/10.1037/0033-2909.97.3.562

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Mazurek, G., & Małagocka, K. (2019). What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think. *Business Horizons*, *62*(6), 751–759. https://doi.org/10.1016/j.bushor.2019.07.008

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*, *4*(1), 1–17. https://doi.org/10.4018/jeco.2006010101

Metzger, M. J. (2007). Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

Micali, S., & Rivest, R. L. (2002). Micropayments Revisited. In B. Preneel (Ed.), *Topics in Cryptology—CT-RSA 2002* (Vol. 2271, pp. 149–163). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45760-7_11

Milne, G. R., & Bahl, S. (2010). Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis. *Journal of Public Policy & Marketing*, *29*(1), 138–149. https://www.jstor.org/stable/20798403

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs*, *51*(1), 133–161. https://doi.org/10.1111/joca.12111

Miyazaki, A. D. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy & Marketing*, *27*(1), 19–33. https://doi.org/10.1509/jppm.27.1.19

Nill, A., & Aalberts, R. J. (2014). Legal and Ethical Challenges of Online Behavioral Targeting in Advertising. *Journal of Current Issues & Research in Advertising*, *35*(2), 126–146. https://doi.org/10.1080/10641734.2014.899529

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

O'Flaherty, K. (2022, February 19). *Allow App To Track On Your iPhone—Here's What It Means*. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2021/11/13/allow-app-to-track-on-your-iphone-heres-what-it-means/

Patel, H. (2022, January 4). *Council Post: How The Delayed Death Of The Cookie Could Impact Advertisers, Publishers And Consumers*. Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2022/01/04/how-the-delayed-death-of-the-cookie-could-impact-advertisers-publishers-and-consumers/

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Reddy, S., Estrin, D., Hansen, M., & Srivastava, M. (2010). Examining micro-payments for participatory sensing data collections. *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, 33–36. https://doi.org/10.1145/1864349.1864355

Rivest, R. L. (1997). Electronic lottery tickets as micropayments. In R. Hirschfeld (Ed.), *Financial Cryptography* (pp. 307–314). https://doi.org/10.1007/3-540-63594-7_87

Rivest, R. L. (2004). Peppercoin Micropayments. In A. Juels (Ed.), *Financial Cryptography* (Vol. 3110, pp. 2–8). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-27809-2_2

Robinson, C. (2017). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582. https://doi.org/10.1016/j.tele.2016.09.006

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2018). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 340–351. https://doi.org/10.1145/3321705.3329806

Saunders, M. N. K. (2015). *Research Methods for Business Students*. Pearson Education UK. http://ebookcentral.proquest.com/lib/bilibrary/detail.action?docID=5138717

Schmidt, D., C. (2018). *Google Data Collection* (pp. 1–55). https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

Schuman, H., & Presser, S. (1996). *Questions and Answers in Attitude Surveys: Experiments on Question Form, Wording, and Context*. SAGE.

Serra, R., & Weyergraf-Serra, C. (1980). *Richard Serra: Interviews, Etc. 1970-1980*. Hudson River Museum.

Shulman, Y., & Meyer, J. (2022). Degrees of Perceived Control Over Personal Information: Effects of Information Relevance and Levels of Processing. *IEEE Access*, *10*, 40596–40608. https://doi.org/10.1109/ACCESS.2022.3167025

Sikt. (n.d.). *Information for participants in research projects*. https://sikt.no/en/information-and-consent

Søndrål, S., & Makin, D. (2020). *What are the implications of using a blockchain-based system for data collection in the insurance industry, where the end-user has ownership of their personal data?* [Master's Thesis]. BI Norwegian Business School.

Strycharz, J., Van Noort, G., Smit, E. G., & Helberger, N. (2019). Consumer View on Personalized Advertising: Overview of Self-Reported Benefits and Concerns. In *Advances in Advertising Research X* (pp. 53–66). Wiesbaden: Springer Fachmedien Wiesbaden.

Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2022). Exploratory Factor Analysis; Concepts and Theory. *Advances in Applied and Pure Mathematics*, *27*, 375–382.

Tam, K. Y., & Ho, S. Y. (2006). Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes. *MIS Quarterly*, *30*(4), 865–890. https://doi.org/10.2307/25148757

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, *9*(3), 203–223. https://doi.org/10.1007/s10660-009-9036-2

The World Bank. (2019, October). *ID4D Practitioner´s Guide: Tamper-proof logs*. The World Bank. https://id4d.worldbank.org/guide/tamper-proof-logs

Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing*, *41*(5/6), 409–418. https://doi.org/10.1108/03090560710737534

Weydert, V., Desmet, P., & Lancelot-Miltgen, C. (2020). Convincing consumers to share personal data: Double-edged effect of offering money. *Journal of Consumer Marketing*, *37*(1), 1–9. https://doi.org/10.1108/JCM-06-2018-2724

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview* (National Institute of Standards and Technology Internal Report 8202; pp. 1–57). http://arxiv.org/abs/1906.11078

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., & Chen, S. (2020). Public and private blockchain in construction business process and information integration. *Automation in Construction*, *118*, 103276. https://doi.org/10.1016/j.autcon.2020.103276

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management*, *47*(2), 115–123. https://doi.org/10.1016/j.im.2009.12.003

Appendices

1. Categories and Items of Digital Personal Data

Socio-Demographic (SD)	
SD1	Demographics (age, gender, ethnicity)
SD2	Professional career (job title, employment history, education history)
SD3	Physical characteristics (picture, height, facial features)
Medical Health (MH)	
MH1	Personal health (diagnoses, health records, prescriptions and medications, physical and mental health)
MH2	Genetic data (genetic information, blood type)
Lifestyle-Behavior (LB)	
LB1	Beliefs (religious, political, philosophical)
LB2	Relationships (family structure, marital status, siblings)
LB3	Interests and preferences (opinions, interests, likes, dislikes)
LB4	Media behavior (web browsing, links clicked, time spent)
Tracking (T)	
T1	Location (GPS location, IP-address, physical address)
T2	Contact information (email address, phone number)
T3	Communication (emails, messages, voice mails)
Authenticating (A)	
A1	Identifiers (Face-ID, fingerprint, ID-number)
A2	Passwords (pin code, passcode, passwords)
A3	Name (first name, last name, username)
Financial (F)	
F1	Financial information (credit card number, annual income, loans)
F2	Purchase habits and history (physical and online)

2. Survey Structure

Q	Measurement	Scale	Variable	Theoretical basis
Block 1: Awareness, Control and Attitude				
Q1	Bipolar 5-point Likert Scale	Strongly disagree; somewhat disagree; Neither agree nor disagree; Somewhat agree; Strongly agree	Ordinal	Self-generated based on Dehling et al. (2019)
Q2	Bipolar 5-point Likert Scale	Strongly disagree; somewhat disagree; Neither agree nor disagree; Somewhat agree; Strongly agree	Ordinal	Self-generated based on Dehling et al. (2019)
Q3	Bipolar 5-point Likert Scale	Strongly disagree; somewhat disagree; Neither agree nor disagree; Somewhat agree; Strongly agree	Ordinal	Self-generated based on Dehling et al. (2019)
Q4	Bipolar 5-point Likert Scale	Strongly disagree; somewhat disagree; Neither agree nor disagree; Somewhat agree; Strongly agree	Ordinal	Self-generated based on Dehling et al. (2019)
Q5	Bipolar 5-point Likert Scale	Strongly disagree; somewhat disagree; Neither agree nor disagree; Somewhat agree; Strongly agree	Ordinal	Self-generated based on Dehling et al. (2019)
Block 2: Willingness to Share				
Q6	Bipolar 5-point Likert Scale	Unwilling; Somewhat unwilling; Undecided; Somewhat willing; Willing	Ordinal	Chua et al., 2021; Gupta et al., 2010; Heirman et al., 2013; Milne et al., 2017; Phelps et al. 2000 & Robinson, 2017.
Block 3: Control on Willingness to Share				
Q7	Bipolar 5-point Likert Scale	Unwilling; Somewhat unwilling; Undecided; Somewhat willing; Willing	Ordinal	Chua et al., 2021; Gupta et al., 2010; Heirman et al., 2013; Milne et al., 2017; Phelps et al. 2000 & Robinson, 2017.
Block 4: Price Sensitivity Meter				
Q8	Price Sensitivity Meter	Range: NOK 0-5 (2 decimal points)	Ratio	Modified Van Westendorp Model (Ceylana et al., 2014)
Q9	Price Sensitivity Meter	Range: NOK 0-5 (2 decimal points)	Ratio	Modified Van Westendorp Model (Ceylana et al., 2014)
Q10	Price Sensitivity Meter	Range: NOK 0-5 (2 decimal points)	Ratio	Modified Van Westendorp Model (Ceylana et al., 2014)
Q11	Price Sensitivity Meter	Range: NOK 0-5N(2 decimal points)	Ratio	Modified Van Westendorp Model (Ceylana et al., 2014)
Block 5: Incentives on Willingness to Share				
Q12	Bipolar 5-point Likert Scale	Unwilling; Somewhat unwilling; Undecided; Somewhat willing; Willing		Chua et al., 2021; Gupta et al., 2010; Heirman et al., 2013; Milne et al., 2017; Phelps et al. 2000 & Robinson, 2017.
Block 6: Demographics				
Q13	Gender: 1-4	Male, Female, Third Gender, Prefer not to say	Nominal	Demographic
Q14	Age: 1-6	18-24; 25-34; 35-44; 45-54; 55-64; 65+	Continuous	Demographic
Q15	Occupation: 1-7	Student; Student with a part-time position; Unemployed; Part-time employee; Full time employee; Self-employed; Retired; Other	Nominal	Demographic
Q16	Country:	List of countries	Nominal	Demographic
Q17	Final comment	Open text entry		

3. Questionnaire

Dear Respondent,
This study is part of our Master Thesis in Strategic Marketing Management at BI Norwegian Business School. The purpose of this study is to get an understanding about the general populations´ willingness to share personal data online with companies for marketing purposes. You do not need to have any prior knowledge on the subject to participate in this study, we only ask you to answer based on your current understanding and initial reactions to the questions. The survey will take approximately 5-10 minutes to complete, and you can withdraw from the questionnaire at any time.

No personally traceable information will be obtained throughout this study, and you will remain completely anonymous. Your responses will be deleted after the completion of this project. Please read the statements below and indicate whether you consent:
- I am 18 years or older
- I have read and understood the general purpose of this project
- I voluntarily take part in this study
- I understand that I can withdraw from the study at any time without any penalty
- I understand that my responses are anonymous

If you have any questions regarding this survey or the data we collect, please contact
Guro Klevrud at gklevrud@gmail.com
Martine Gulstad at martine.gulstad@gmail.com
We thank you for your participation!

I agree with the statement of informed consent listed above

- ○ Yes, I agree
- ○ No, I do not agree

Online Behavioral Advertising

In the first section of the study we ask you to rate the degree to which you agree with the following statements. There are no right or wrong answers. Please answer the questions based on your current knowledge or beliefs about the topic.

I am aware of which digital personal data is collected about me when I visit and use online webpages and services

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
○	○	○	○	○

I understand how companies use my digital data to create and reach me with personalized ads, content and communication

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
○	○	○	○	○

I am not in control of the collection and use of my digital personal data

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
○	○	○	○	○

I become suspicious when I receive digital advertisements that are customized to my interests

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
○	○	○	○	○

I find personalised advertisements to be useful

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
○	○	○	○	○

Consumer Willingness to Share Digital Personal Data

When we use digital services, we often allow companies to collect certain types of personal information, for example by accepting cookies on a website. This information is called personal data, which can later be used to create and reach you with personal offers, content, communication and advertisements.

In this section we ask you to evaluate your own willingness to share different types of personal data with companies for such marketing purposes. There are no correct or incorrect answers, we simply ask you to rate your willingness based on your initial reaction and evaluation.

How willing are you to share the following types of personal data with companies online for marketing purposes?

	Unwilling	Somewhat unwilling	Undecided	Somewhat willing	Willing
Demographics (age, gender, ethnicity)	○	○	○	○	○
Professional career (job title, employment history, education history)	○	○	○	○	○
Physical characteristics (picture, height, facial features)	○	○	○	○	○
Personal health (diagnoses, health records, prescriptions and medications, physical and mental health)	○	○	○	○	○
Genetic data (genetic information, blood type)	○	○	○	○	○
Beliefs (religious, political, philosophical)	○	○	○	○	○
Relationships (family structure, marital status, siblings)	○	○	○	○	○
Interests and preferences (opinions, interests, likes, dislikes)	○	○	○	○	○

	Unwilling	Somewhat unwilling	Undecided	Somewhat willing	Willing
Media behavior (web browsing, links clicked, time spent)	○	○	○	○	○
Location (GPS location, IP-address, pyhsical address)	○	○	○	○	○
Contact information (email address, phone number)	○	○	○	○	○
Communication (emails, messages, voice mails)	○	○	○	○	○
Identifiers (Face-ID, fingerprint, ID-number)	○	○	○	○	○
Passwords (pin code, passcode, passwords)	○	○	○	○	○
Name (first name, last name, username)	○	○	○	○	○
Financial information (credit card number, annual income, loans)	○	○	○	○	○
Purchase habits and history (physical and online)	○	○	○	○	○

Control: Consumer Willingness to Share Digital Personal Data

We now introduce a scenario where you have complete control of your own data. With new technology, you can now share data directly with companies and decide what type of information you would like to share. In this scenario, you will have access to insight about who can access your data, and you have the right to withdraw your information at any time. The data you choose to share will be used to provide you with personalized offers, discounts, content, and advertisement from that specific company.

An example of this scenario is that you share your purchase history with an online fashion company, and later receive news letters and discounts from the same company for similar products that match the style of your previous purchases.

Given this scenario we now ask you to evaluate your willingness to share the different types of personal data with companies for such marketing purposes. There are no correct or incorrect answers, we simply ask you to rate your willingness based on your initial reaction and evaluation.

In a scenario where you are in complete control of your own data, how willing are you to share the following types of personal data with companies online for marketing purposes?

	Unwilling	Somewhat unwilling	Undecided	Somewhat willing	Willing
Demographics (age, gender, ethnicity)	○	○	○	○	○
Professional career (job title, employment history, education history)	○	○	○	○	○
Physical characteristics (picture, height, facial features)	○	○	○	○	○
Personal health (diagnoses, health records, prescriptions and medications, physical and mental health)	○	○	○	○	○
Genetic data (genetic information, blood type)	○	○	○	○	○
Beliefs (religious, political, philosophical)	○	○	○	○	○
Relationships (family structure, marital status, siblings)	○	○	○	○	○

	Unwilling	Somewhat unwilling	Undecided	Somewhat willing	Willing
Interests and preferences (opinions, interests, likes, dislikes)	○	○	○	○	○
Media behavior (web browsing, links clicked, time spent)	○	○	○	○	○
Location (GPS location, IP-address, physical address)	○	○	○	○	○
Contact information (email address, phone number)	○	○	○	○	○
Communication (emails, messages, voice mails)	○	○	○	○	○
Identifiers (Face-ID, fingerprint, ID-number)	○	○	○	○	○
Passwords (pin code, passcode, passwords)	○	○	○	○	○
Name (first name, last name, username)	○	○	○	○	○
Financial information (credit card number, annual income, loans)	○	○	○	○	○
Purchase habits and history (physical and online)	○	○	○	○	○

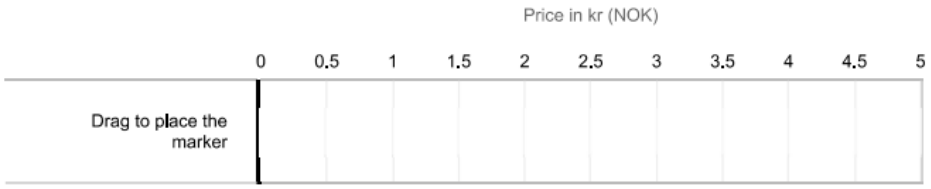
Van Westendorp Price Sensitivity Meter

Building on the previous scenario, we would like to explore a new scenario where the data you decide to share with companies is rewarded with a small payment. You are still in complete control of your own data, and you can withdraw the information you have shared at any time.

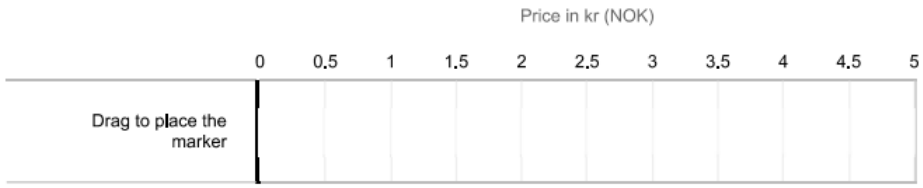
An example of this scenario can be a music streaming platform that offers you a reward system for sharing data on your streaming and listening habits. For every 25 songs you listen to, you are rewarded a small payment for allowing the platform to collect data on the song titles and the artists' names. The collected data can then be used to provide you with new music recommendations, artist promotions or advertisements.

We now ask you to evaluate different price points of the payment you would receive by allowing the music streaming platform to collect data on every 25 songs you listen to. Assume such payments will be in the range of (NOK) 0-5kr (about USD 0-0.5) each time the data is collected or used.

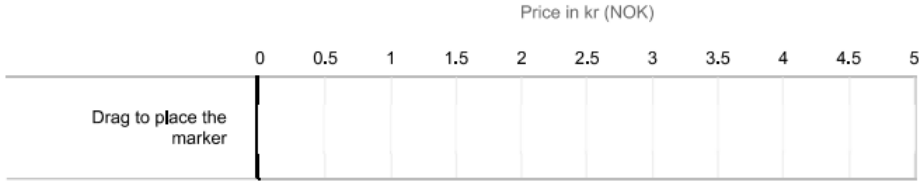
At what price would you consider the payment to be so low that sharing your information would not be worth it?



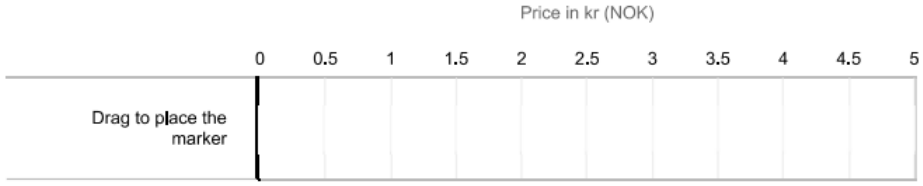
At what price do you consider the payment for sharing your information to be so high you become suspicious of the buyer´s intentions?



At what price do you consider the payment to be low but still high enough so that you would start considering sharing your information?



At what price would you consider the payment to be a good deal for sharing your information without becoming suspicious of the buyer´s intentions?



ıcentives & Control: Consumer Willingness to Share Digital Personal Data

Considering the previous scenario where you are in complete control of your own data and receive a small payment for sharing information, we again ask you to evaluate your willlingness to share the different types of personal data with companies for marketing purposes. There are no correct or incorrect answers, we simply ask you to rate your willingness based on your initial reaction and evaluation.

In a scenario where you are in complete control of your data, and receive a small payment for sharing information, how willing are you to share the following types of personal data with companies online for marketing purposes?

	Unwilling	Somewhat unwilling	Undecided	Somewhat willing	Willing
Demographics (age, gender, ethnicity)	○	○	○	○	○
Professional career (job title, employment history, education history)	○	○	○	○	○
Physical characteristics (picture, height, facial features)	○	○	○	○	○
Personal health (diagnoses, health records, prescriptions and medications, physical and mental health)	○	○	○	○	○
Genetic data (genetic information, blood type)	○	○	○	○	○
Beliefs (religious, political, philosophical)	○	○	○	○	○
Relationships (family structure, marital status, siblings)	○	○	○	○	○
Interests and preferences (opinions, interests, likes, dislikes)	○	○	○	○	○
Media behavior (web browsing, links clicked, time spent)	○	○	○	○	○
Location (GPS location, IP-address, physical address)	○	○	○	○	○
Contact information (email address, phone number)	○	○	○	○	○
Communication (emails, messages, voice mails)	○	○	○	○	○
Identifiers (Face-ID, fingerprint, ID-number)	○	○	○	○	○
Passwords (pin code, passcode, passwords)	○	○	○	○	○
Name (first name, last name, username)	○	○	○	○	○
Financial information (credit card number, annual income, loans)	○	○	○	○	○
Purchase habits and history (physical and online)	○	○	○	○	○

Demographics

To gain a better understanding of our respondents, we ask you to provide some basic information about yourself in the last section of this survey.

Gender

- ○ Male
- ○ Female
- ○ Non-binary / third gender
- ○ Prefer not to say

Age

- ○ 18-24
- ○ 25-34
- ○ 35-44
- ○ 45-54
- ○ 55-64
- ○ 65+

Occupation

- ○ Student
- ○ Student with a part-time position
- ○ Unemployed
- ○ Part-time employee
- ○ Full time employee
- ○ Self-employed
- ○ Retired
- ○ Other

In which country do you currently live?

Is there anything you would like to add or comment on regarding this survey?

4. Correlation Matrix for Category Items

		Socio-Demographic			Medical Health		Lifestyle-Behavior				Tracking			Authenticating			Financial	
	Item	1	2	3	1	2	1	2	3	4	1	2	3	1	2	3	1	2
Socio-Demographic	1																	
	2	.53***																
	3	.35***	.54***															
Medical Health	1	.24***	.32***	.43***														
	2	.18***	.25***	.39***	.69***													
Lifestyle-Behavior	1	.48***	.48***	.36***	.34***	.44***												
	2	.45***	.52***	.42***	.34***	.41***	.55***											
	3	.54***	.50***	.27***	.20***	.26***	.50***	.55***										
	4	.45***	.42***	.22***	.14**	.20***	.40***	.47***	.66***									
Tracking	1	.27***	.33***	.31***	.25***	.27***	.30***	.42***	.38***	.42***								
	2	.28***	.22***	.31***	.22***	.26***	.28***	.33***	.29***	.23***	.36***							
	3	.20***	.14**	.24***	.26***	.29***	.16**	.35***	.20***	.21***	.36***	.59***						
Authenticating	1	.11	.21***	.26***	.32***	.18**	.18**	.24***	.22***	.16**	.27***	.29***	.39***					
	2	.05	.12	.20***	.19***	.12	.16**	.13	.07	.06	.12	.15**	.28***	.57***				
	3	.35***	.35***	.32***	.15**	.18***	.33***	.44***	.45***	.44***	.36***	.51***	.4***	.38***	.29***			
Financial	1	.13	.26***	.27***	.23***	.18**	.16**	.16**	.07	.15**	.18**	.28***	.36***	.42***	.51***	.36***		
	2	.43***	.33***	.23***	.21***	.19***	.35***	.32***	.43***	.60***	.32***	.30***	.27***	.27***	.20***	.48***	.28***	

***Significant at the .01 level (two-tailed)
**Significant at the .05 level (two-tailed)

5. Path Diagram of Digital Personal Data Categories