



Norwegian University of Life Sciences  
School of Economics and Business

Philosophiae Doctor (PhD)  
Thesis 2023:25

# Four Papers on Privacy and Human Behavior

Fire artikler om personvern og adferd

Ole Christian Berg Wasenden



# Four Papers on Privacy and Human Behavior

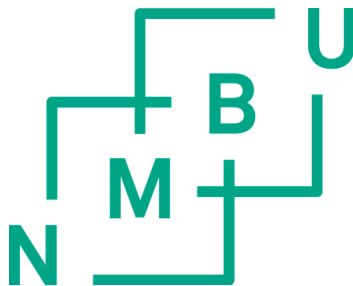
Fire artikler om personvern og adferd

Philosophiae Doctor (PhD) Thesis

Ole Christian Berg Wasenden

Norwegian University of Life Sciences  
School of Economics and Business

Ås (2023)



Thesis number 2023:25  
ISSN 1894-6402  
ISBN 978-82-575-2055-7





*“If this is the age of information, then privacy is the issue of our times.”*

Acquisti et al. (2015)



## Acknowledgments

This PhD thesis is the result of a collaborative project between my employer, Telenor Research and Innovation, and the School of Economics and Business at the Norwegian University of Life Sciences. The project, entitled "Consumer Choice, Personal Data and Privacy in the Smartphone Age," was funded by the Research Council of Norway and Telenor. I am grateful to Telenor for their support throughout the project and to the School of Economics and Business for allowing me to pursue my doctoral studies and welcoming me into their academic community. I would also like to express my gratitude to the Research Council of Norway, and particularly the Industrial PhD program, without which this project would not have been possible.

I am also very grateful for all the support I have received from Frode, my main supervisor. You have remained calm, patient, and supportive throughout the process, and have always been available when I needed guidance. An internal supervisor is a mandatory part of doing an industrial PhD, and I have had three. Eleonora took over and did the longest and hardest leg of the race. Thank you for always being positive, for clear feedback and a structured approach. Thanks also to Bjørn-Atle who kicked me off, and to Simen, for pushing me up the last hill. Ceren, who has co-authored one of the papers and has been an important discussion partner, both regarding the thesis but also on a wide variety of other topics, deserves a special thank you.

I have spent around 20 years in the various versions of the research department at Telenor. Working with so many inspiring colleagues over the years helped me mature the idea of starting a PhD project. In random order (yes, I actually used a randomizer) Wenche, Helene, Bjørn, Dagfinn, Gorm, Kjetil, Rich, Bjørn-Taale, and Bente, you have all played a part that I am grateful for.

Luckily, there is a life outside a PhD project. Sigurd, Åshild, and Ingrid, my fantastic children. I will not even try to put into words how much you mean to me. Thank you for being you. Mum and dad. In this context I would like to thank you both for being great inspirations. One of you handed in a PhD thesis just before turning 60, and the other was headhunted by big tech at that age, because you knew their stuff better than they did themselves. And Odd-Harald, my brother, thanks for having my back and taking the time when I make the "I need to talk" call.

Finally, for all good friends, I will use the "none mentioned, none forgotten" trick. Thank you for not giving up on me. There have been some "no, sorry, maybe next time" answers from my side, and I plan to change that.



# Contents

Acknowledgments . . . . .	1
Contents . . . . .	3
List of papers . . . . .	5
Summary . . . . .	7
Sammendrag . . . . .	9
<b>Introduction</b>	<b>11</b>
Background and motivation . . . . .	11
Literature . . . . .	15
Data . . . . .	22
Paper summaries . . . . .	24
Concluding remarks . . . . .	30
References . . . . .	33
<b>Paper 1</b>	<b>37</b>
<b>Paper 2</b>	<b>49</b>
<b>Paper 3</b>	<b>61</b>
<b>Paper 4</b>	<b>109</b>
<b>Appendix: Paper 1 - English translation</b>	<b>157</b>



# List of papers

1. **Digitalt personvern - kunnskap, bekymring og adferd** (Digital Privacy - Knowledge, Concern, and Behavior. English version in Appendix)  
Author: Ole Christian Wasenden  
Published in *Magma*
2. **Your privacy for a discount? Exploring willingness to share personal data in return for personalized offers**  
Authors: Frode Alfnes and Ole Christian Wasenden  
Published in *Telecommunications Policy*
3. **Privacy during Pandemics: Attitudes to Public Use of Personal Data**  
Authors: Eleonora Freddi and Ole Christian Wasenden
4. **Information Avoidance and Privacy — the role of Entertaining Content**  
Authors: Fehime Ceren Ay, Eleonora Freddi, and Ole Christian Wasenden





# Summary

This thesis examines the decision-making process and preferences relating to digital privacy. The four articles investigate questions such as: How do we make decisions when sharing our data with a third party, commercial or public? Do we really care about privacy, or are we indifferent? When are we willing to trade our personal data for a benefit?

The first paper studies privacy from a customer perspective through a two-wave survey conducted in 2017 and 2018 among young Norwegians. We assess their awareness of digital privacy, measured by levels of concern about and knowledge of privacy. We then looked at how this awareness affected privacy behavior. In spring 2018, the introduction of the EU's new General Data Protection Regulation (GDPR) and what became known as the "Cambridge Analytica scandal" received a lot of media attention. Our analysis revealed a significant increase in privacy knowledge during this period, while the level of concern was high. Many take active steps to protect their data, and this is correlated with high concern and knowledge.

In the second paper, we investigate the willingness of young mobile users in Malaysia, Norway, Pakistan, and Serbia to share personal data in return for receiving personalized ads on their cell phones. We test whether the likelihood of using such an ad service varies with the level of personal data collected and whether data are shared with third parties. The likelihood decreases when the service uses more personal data. Further, we find that, in three of the four countries, giving a 10% discount on cell phone subscriptions for using the ad service increases the stated likelihood of using the service. Respondents in Norway were least willing, while those in Pakistan were most willing to share personal data.

The third paper examines people's attitudes to sharing personal data when the data are used to help society combat a serious contagious disease. Through a two-wave survey, in 2020, conducted in Norway and Sweden, we investigate the role of personal characteristics, and the effect of information, in shaping attitudes to privacy. We find that privacy concern is negatively correlated

with allowing public use of personal data. Trust in the entity collecting the data and collectivist preferences are positively correlated with this type of data usage. Providing more information about the health benefit of sharing personal data makes respondents more positive, while providing additional information about the privacy costs does not change attitudes. Stating a clear purpose for the data collection makes respondents more positive about sharing. In a comparison across survey waves and countries, we find that our results are robust across contexts and policy choices.

In the fourth paper we presents new insights into the relationship between hedonic well-being, privacy decisions, and information avoidance. We investigate the tendency of individuals to avoid privacy information when they are exposed to entertaining online content. Consuming such content can lead to high levels of hedonic well-being, making it more likely that privacy information could have a negative effect. In an online experiment, we show participants online, and they must either seek out or avoid information about privacy. The entertainment value of the videos and the indicated time cost of obtaining the privacy information are varied. We found that the entertainment value of the videos and the time cost had weak negative effects on information seeking. Our findings also indicate that participants who were exposed to entertaining content anticipated a more negative impact of privacy information on their user experience.

This thesis contributes with new insights into privacy, human behavior and the sharing of personal data in digital everyday life. The survey data are collected in countries that vary greatly in terms of both their technological and economic development, and in relation to attitudes to privacy and its status in law. Despite these differences, similarities are evident across the different contexts in the four articles. Firstly, we see that many respondents are concerned about their privacy when online. Furthermore, high levels of concern are accompanied by lower willingness to share data, while the opposite is the case for trust in the actor who collects the data. The findings pave the way for more research on privacy and human behavior.

## Sammendrag

I denne avhandlingen belyses privatpersoners beslutningsprosesser og preferanser knyttet til digitalt personvern. Gjennom fire artikler søkes svar på spørsmål som: Hvordan tar vi beslutninger når vi deler dataene våre med en tredjepart, kommersiell eller offentlig? Bryr vi oss virkelig om personvern, eller er vi likegyldige? Når er vi villige til å bytte bort våre personlige våre?

Den første artikkelen studerer personvern fra et kundeperspektiv gjennom en spørreundersøkelse utført blant unge nordmenn i to runder i 2017 og 2018. Vi ser nærmere på deres bevissthet om digitalt personvern, målt gjennom bekymrings- og kunnskapsnivå. Vi ser videre på hvordan denne bevisstheten påvirker personvernadferd. Våren 2018 fikk innføringen av EUs nye personvernregulering og den såkalte “Cambridge Analytica”-skandalen mye omtale i mediene. Vår undersøkelse avdekket betydelig økning i personvern-kunnskap i denne perioden, mens bekymringsnivået var høyt. Mange tar aktive grep for å beskytte dataene sine, og dette er korrelert med høy bekymring og kunnskap.

I den andre artikkelen undersøker hvor villige unge mobilbrukere i Malaysia, Norge, Pakistan og Serbia er til å dele personlige data for å motta personlig tilpassede annonser på mobiltelefonene sine. Vi tester om villigheten til å bruke en slik annonsetjeneste varierer med hvor mye personlige data som samles inn og om disse deles med tredjeparter. Vi finner at villigheten reduseres når tjenesten bruker mer data. Videre finner vi at i tre av de fire landene øker villigheten til å bruke tjenesten ved å tilby en 10% rabatt på mobilabonnement. Respondentene i Norge var minst villige til å dele sine personlige data mens de i Pakistan var mest villige.

Den tredje artikkelen undersøker folks holdninger til å dele personlige data med helsemyndighetene når dataene brukes til å hjelpe samfunnet med å bekjempe en alvorlig smittsom sykdom. Gjennom en undersøkelse gjennomført i Norge og Sverige i to bølger i 2020, studerer vi hvordan personlige karakteristika og det å gi ulik informasjon påvirker holdninger til personvern. Vi finner at bekymring knyttet til personvern er negativt korrelert med å tillate offentlig bruk av personlige

data. Tillit til aktøren som samler inn dataene og kollektivistiske preferanser er positivt korrelert. Å gi informasjon om helsegevinsten ved å dele sine personlige data gjør respondentene mer positive, men vi finner ingen signifikant endring ved å gi informasjon om ulemper ved å oppgi sine data. Å være tydelig på hvilket formål en har med datainnsamlingen gjør respondentene mer positive til deling. I en sammenligning på tvers av de to rundene og landene finner vi at resultatene våre er robuste på tvers av kontekster og politiske valg.

I den fjerde artikkelen presenterer vi ny innsikt knyttet til forholdet mellom hedonisk velvære, personvernadferd og hvorvidt man unngår informasjon. Vi undersøker om det å konsumere innhold med høy underholdningsverdi øker sannsynligheten for at personverninformasjon unngås. Å konsumere slikt innhold vil ofte gi høy hedonisk velvære, noe som kan gjøre det mer sannsynlig at personverninformasjon kan ha en negativ effekt. I et netteksperiment viser vi deltakerne to videoer med ulik underholdningsverdi. Mellom videoene må de beslutte om de vil gå inn og lese personverninformasjon eller ikke. Deltagerne fikk også ulike anslag på hvor lang tid det ville ta å lese informasjonen. Vi fant at både underholdningsverdi og tidskostnaden hadde svake negative effekter på om informasjonen ble lest. Funnene indikerer også at deltakere som så underholdende videoer i større grad forventet at personverninformasjon ville ha en negativ effekt på deres brukeropplevelse.

Denne avhandlingen bidrar med ny innsikt om menneskelig adferd knyttet til personvern og hvordan vi deler personlige data i vår digitale hverdag. Dataene er samlet inn i land med ulik teknologisk og økonomisk utvikling, og med betydelige forskjeller i holdninger til personvern og personvernregulering. Til tross for disse forskjellene er det tydelige likheter på tvers de ulike kontekstene i de fire artiklene. For det første ser vi at mange respondenter har bekymringer knyttet til personvern når de er på nett. Videre er høy grad av bekymring ledsaget av lavere vilje til å dele data, mens det motsatte er tilfellet hvis man har tillit til aktøren som samler inn dataene. Funnene baner vei for mer forskning på personvern og menneskelig adferd.

# Introduction

## 1.1 Background and motivation

Privacy is the subject of lively debate both in society in general and among scholars. It has frequently been claimed both that privacy is dead, due to the overwhelming amounts of personal data that are generated, collected, stored, and used when online, and also that this calls for action to strengthen the protection of privacy even more (Acquisti et al., 2015; Dienlin and Breuer, 2022). This thesis contributes with new insights into privacy, human behavior, and the sharing of personal data in digital everyday life.

In 2018 the new General Data Protection Regulation (GDPR) entered into force, as the most ambitious privacy regulation globally.<sup>1</sup> During the period before its implementation, businesses devoted a lot of resources to preparing for the new regulations. At the same time, using personal data to personalize services was seen as a logical way of developing businesses. For businesses, there was a risk of ending up in a situation where using as much personal data as possible was seen as a necessity, defining privacy as nothing more than a legal issue, and consequently forgetting about their customers' preferences. That was the starting point for the work on this thesis; to gain a better understanding of customer preferences when using a service from a service provider that collects and uses their personal data.

Privacy in combination with technological development is not a new topic, however, as illustrated by Warren and Brandeis (1890): “*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechan-*

---

<sup>1</sup><https://gdpr.eu/what-is-gdpr/>

*ical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"*. This quote from the seminal paper in *Harvard Law Review* is perfect for reflecting on privacy today as well. It provides a simple definition that is still very relevant today: privacy can be seen as the *right to be left alone*. Secondly, it tells us that media and technology constituted a threat to privacy already 130 years ago, and that there was a need for laws to protect it. It is also interesting that the authors emphasise that the problems were caused by mechanical devices, so that, even though this was in truly pre-digital times, the invention of new things, like a camera, became a threat to privacy.

In 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights (United Nations, 1948), a declaration that included the right to privacy in one of its articles. A similar privacy element is a part of the European Convention on Human Rights (Council of Europe, 1950). Despite having been a human right for more than 70 years, there is no generally accepted definition of the term, and, when drafting the human rights declarations, no attempt was made to define it clearly (Diggelmann and Cleis, 2014). According to Whitman (2003), there are two main ideas; the first follows Warren and Brandeis (1890) who state that privacy is the right to be left alone or *privacy as freedom from society or the state*, while the second is the right to keep control of your own information, such as your image, name, and reputation, or *privacy as dignity*. Which of these concepts is most relevant will depend on the context and also the culture. The first is close to the American idea that the state should let the individual alone, while the latter is closer to the European idea of privacy.

In relation to the contextual dimension, the right to be left alone would, for example, be relevant in a setting with state surveillance. The so-called "Snowden revelations" showed how the US National Security Agency used data from internet companies like Facebook and Google and phone logs from Verizon for mass surveillance purposes, also of US citizens (Lyon, 2014). It was documented that state agencies in the US, but also in the UK and Canada, surveilled their populations on a large scale. The second definition might be more relevant to situations in which an individual discloses personal data when using an online service, but the two are interlinked. All the individual transactions together make up big data sets that could potentially facilitate mass surveillance.

In addition to the potential privacy challenges of the relationship between the state and the citizen, there is a plethora of potential challenges in the business-customer dimension. Amnesty

International (2019) highlights such a challenge in its report “Surveillance giants: How the business model of Google and Facebook threatens human rights”, stating that the business models of companies like Facebook and Google represent an unprecedented threat to human rights. The technological development, with internet available everywhere, fast mobile connections, powerful smartphones, and more and more gadgets connected to the internet of things, has changed the way in which we live our lives. The changes have happened quickly, and only 20 years ago, cell phones were mainly used for communication purposes, and not everyone had one. Today, such phones are used for a wide range of purposes and are always switched on.

As internet usage and digital interactions are becoming omnipresent, digital privacy is being increasingly challenged. We spend more time online and use a wider range of services, the amount of personal data that is collected has grown significantly. Keeping track of how the data are used has become increasingly challenging. In many cases, personal data are the “price” we pay for using a service. Kummer and Schulte (2019) study the money-for-privacy trade-off in the app universe. They describe the balancing act that companies, governments, and consumers must perform. Enough data should be used to create good services that can increase welfare, but, on the other hand, the services should not collect so much data that they become intrusive or use data for negative purposes in a way that is unclear to those whose data are being used. They study 300 000 apps on Google Play, and find that prices are generally lower for apps that collect more data. They also find that demand for apps decreases with how much data they collect. Finally, they find that this negative relationship between demand for an app and data greediness is context-dependent, and that factors such as trust and type of app play a role.

The relationship between data collection and demand for apps and services is complex, and the balance between providing valuable services and protecting privacy is a key concern. This thesis looks at this topic from the perspective of the individual, examining the decision-making process and preferences concerning the sharing of personal data with third parties. Through four papers, my co-authors and I investigate questions such as: How would we like our personal data to be treated? How do we make decisions when sharing our data with a third party, commercial or public? Do we really care, or are we indifferent? When are we willing to trade our personal data for a benefit? The four papers examine various aspects of privacy, using survey and experimental data from three continents. We look into trust, privacy concerns, and knowledge, commercial

and public data collectors and the role of privacy information, and explore potential effects on behavior.

In *Paper 1*, We study privacy attitudes and protective actions among young Norwegians, through a two-wave survey conducted in 2017 and 2018. The purpose of conducting the second wave of the survey was to examine the impact of two major privacy events that occurred during spring 2018: the Cambridge Analytica scandal and the introduction of the General Data Protection Regulation (GDPR). These events received significant media attention and had a potential impact on privacy knowledge and attitudes. The findings show that young Norwegians care about privacy and take actions to protect it, and that there was an increase in privacy knowledge between the two waves.

*Paper 2* looks at the value of privacy in a personalized marketing context. Through a survey experiment, respondents in four countries, Malaysia, Norway, Pakistan, and Serbia, were asked whether they would use a service in which they receive personalized ads based on data from their mobile phones. A randomized half of the sample were given a 10 percent discount on their cell phone bill, if they accepted using the service. The level of personal data collected also varied. In three of four countries, we find an increase in willingness to use the personalized ads when the discount is given. We also see that the willingness decreases when the service collects more data.

*Paper 3* investigates people's willingness to share data with health authorities in order to combat a serious contagious disease. Through a two-wave survey in Norway and Sweden, we endeavor to gain a better understanding attitudes to data sharing. High trust and collectivist preferences are accompanied by more positive attitudes, while the opposite is the case for high levels of privacy concern. More information on the public benefit and stating a clear purpose makes the respondents more positive about the use of their data. We also find that our results are robust across contexts and policy choices.

*Paper 4* combines two distinct but complementary fields of economics, one concerning privacy and the other concerning information avoidance, and we examine whether people exposed to highly entertaining online content are more likely to avoid privacy information. We run an experiment on the crowdsourcing platform Prolific, with participants from the US and Canada, where participants must seek out or avoid privacy information in a situation where they watch videos online. How entertaining the videos are, and the indicated time cost of accessing the information is randomly varied. We find weak negative effects on information seeking of variations in the



entertainment level and time cost.

In the following, I will first provide an overview of relevant literature and briefly connect the papers to the literature. This will be followed by an overview of the data used in the various papers, and by more detailed summaries of the four papers. Finally, some concluding remarks are included.

## Literature

The economic literature on privacy is growing, and in the survey article *The economics of privacy*, (Acquisti et al., 2016) conclude that privacy-related questions are relevant in many different economic contexts. It is therefore not straightforward to establish one unifying theory of privacy. Despite this, they define the economic study of privacy as a sub-field of information economics. Even though privacy is a wide term with different definitions, information is at its center. They find that, given the circumstances, keeping personal information private could both enhance and decrease private and societal welfare, and that it is not possible to say that keeping personal information private would be either positive or negative. In one case, individuals could benefit from protecting their privacy, while, in another, they could benefit from sharing data with someone because the interaction with the entity that receives the data becomes more valuable.

Acquisti et al. (2016) approach the subject of privacy from both a theoretical and empirical perspective. On the theoretical side, they focus on the level of regulation. One possibility is to have no regulation at all, leaving everything to the interaction between the consumer and the firm (or the user and the entity that asks for data in more general terms). A second possible way is to have laws that establish clear ownership, and facilitate free trade in data. Thirdly, regulation could be stricter, with strong protection of personal data that might make use more difficult. The empirical economics literature is mainly about the trade-off between the benefit that might be gained by giving up data and the risk or cost of reduced privacy. They list a range of areas where such trade-offs exist, including *Advertising and Electronic Commerce*, *Price Discrimination*, *Health Economics*, *Markets for Privacy and Personal Data*, *Privacy and Information Security*, and *Consumer Attitudes and Behaviors*.

In Figure 1.1, I include a non-exhaustive set of topics where privacy is relevant, and that partly overlap with those listed by Acquisti et al. (2016). It serves as an illustration of the com-

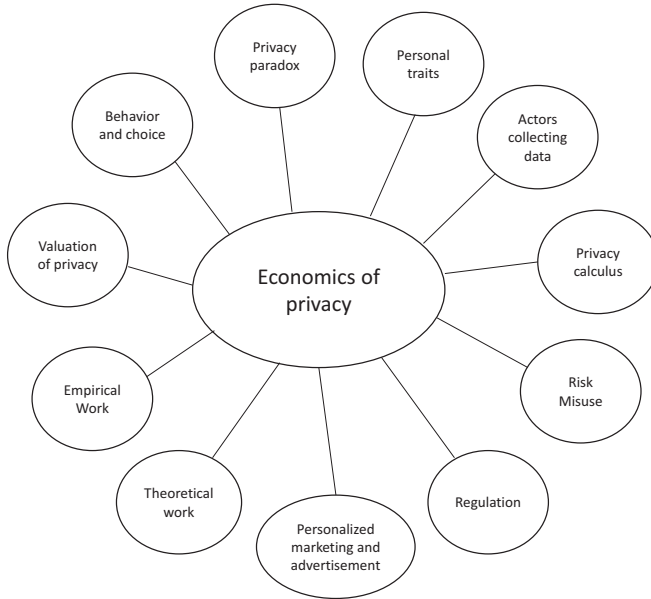


Figure 1.1: Economics of privacy - some important elements

plexity of privacy considerations in the economic literature. In the remainder of this section, I will delve deeper into the literature related to the key sub-topics of this thesis. They are: “Privacy preferences and behavior”, “Valuation of personal data and privacy”, “Personalized marketing and advertisements”, “Regulation and consent”, and “Privacy in health care and crises”. Finally, some elements from information economics, relevant to the thesis, are presented. These topics are not mutually exclusive, and there are papers that would fit several of them, but they help to sort the wide variety of topics covered in the economic literature on privacy.

### 1.1.1 Privacy preferences and behavior

In this section, the main focus is on preferences and behavior in settings in which the individual must decide whether to share personal data to gain some kind of benefit or keep the personal data private and lose the benefit. The benefit could be a better service, a personalized ad, more efficient health care or a payment or money bonus. The growing literature on privacy does not take a uniform view on the formation of privacy preferences and behavior. At the high level,

the views can be sorted into three main categories: the first is that people care and take appropriate actions, the second is that they do not really care, while the third is that people say that they care, but do not act accordingly. The latter is known as the privacy paradox, which Athey et al. (2017) illustrate through an experiment. They find that participants in an experiment are significantly more willing to give up the email addresses of their friends for as little as a pizza, compared to those who are not given the same incentives. They also find that small navigation costs make a significant difference between the stated preference and actual behavior. In this case, it is the default list of options of digital wallets that varies (the privacy experiment is added to a project in which digital money is the main topic), some being more privacy-friendly than others. Irrelevant information and toning down privacy issues are also found to have an effect on behavior, and could make participants less protective of personal information. Kokolakis (2017) reviews the literature on the privacy paradox, and finds no consensus on whether there is such a paradox between stated concerns and actions to protect privacy. In the first paper in this thesis, we study privacy concerns and actions among young Norwegians, and do not find support for the paradox.

Acquisti et al. (2020) review the literature on consumers' privacy decision-making and find that consumers care fundamentally about privacy, are concerned about it, and take actions to protect it. However, they find that it is very difficult for consumers to achieve the desired level of privacy. Different psychological factors play a role, such as present bias, adaptation (doing what others do), and the drive to share information while online. Moreover, information asymmetries between firms collecting data and consumers sharing their data might give the firms an advantage. They conclude that protecting privacy is prohibitively difficult and recommend stricter regulation to protect privacy. In Papers 1 and 2, we measure privacy knowledge levels and use this in our analysis of behavior.

Privacy choices are quite often made in steps. For example, when using social media, you first decide on your privacy settings, with whom you share what, and then, secondly, decide on what to actually post on your wall or profile page. Similarly, when carrying out an online search, you first decide on the search engine and after that conduct the actual search. Adjerid et al. (2019) study how the choice architecture of such sequential choices could affect the final outcomes. Most research has been done on the downstream level, what is actually shared, and less on the upstream settings. We study what can be seen as a third level of the privacy choice architecture in the fourth paper, on information avoidance. Consumers frequently have to choose between learning details

about privacy settings or not before they start to use a service, and this layer could be added to a model like the one in Adjerid et al. (2019).

Inattention and lack of awareness could play a major role in privacy choices. Marreiros et al. (2017) study the role of privacy information and the attention consumers pay to it. They expose respondents in a survey experiment to information about how a company will use their data, and test whether this has an effect on their privacy choices. They use content from actual media coverage about privacy practices of firms like Facebook and Dropbox to find out whether being exposed to this information has an effect on privacy choices. They randomly expose the experiment participants to negative, neutral, or positive privacy practices. Then they test how willing respondents are to share personal information, their attitudes to social action (donating to an advocacy group), and stated privacy preferences. Interestingly, they find that there are no differences in willingness to share personal data between those primed with positive privacy information compared to those primed with negative information. Both these groups are significantly less willing to share data than the group that is primed with neutral privacy information. This indicates that merely mentioning privacy, regardless of whether the information is positive or negative, makes people aware of privacy and, as a result, less willing to share. We use a similar method in our third paper, in which we asked individuals to share data with health authorities to combat a serious disease. We expected that providing more information about health benefits would increase willingness to share, while more information about privacy costs would decrease willingness. However, we found that the effects were only significant for the health benefits.

Svirsky (2022) studies information avoidance and privacy behavior. In an experiment, all participants were informed at the beginning that they could take a survey either anonymously or after logging in with their Facebook account at a privacy cost. Giving up privacy would yield a higher payment, so there was a privacy for money trade-off. When making the actual choice, half of the sample were given information about both privacy and payment levels, while, for the other group, the privacy information was hidden behind a “Click here to see the privacy settings” button. In the latter case, which opened for information avoidance, a larger share logged in with their Facebook account, thereby giving up their privacy, than in the group that were given the privacy information by default. Information avoidance and privacy is the topic of the fourth paper in the thesis.

### **1.1.2 Valuation of personal data and privacy**

An understanding of the valuation of protection of personal information is important for businesses, law and public policy (Acquisti et al., 2013), and the literature from this branch of privacy research is also growing. A standard way of finding out how consumers value a good or a service is to look at their willingness to pay (WTP) and willingness to accept (WTA). Winegar and Sunstein (2019) find that a median consumer is willing to pay 5 dollars per month to keep certain specified data private, but would ask for 80 dollars to give up similar data. They find what they call a super-endowment effect, as the standard WTP/WTA ratio is found to be around 1:2. Using MTurk they tested for 8 different specifications and found this effect across all of them. Acquisti et al. (2013) also find a very strong endowment effect for privacy. These findings indicate that it is quite challenging for individuals to put a price on their personal data.

Other research looks at the relative valuation of different items of private information. Using a choice experiment, Savage and Waldman (2015) estimate the willingness to pay for apps that conceal five different types of personal data. They are browser history, location, contacts, phone ID, and content of messages/texts. They conducted in-person interviews with repeated discrete-choice experiments, where participants chose between one app that is free, but collects all data and another that is not free but collects fewer data. The apps are otherwise identical in function. They conclude that participants are able to make the trade-off. Further, they find that participants put a value on all five different data elements, and this value differs across segments such as income and education. On average, the highest value is put on personal contact lists, followed by content of texts and browser history. The valuation of location is relatively low.

In the second paper in the thesis, we use a survey experiment to look at the trade-off between a discount on one's cell phone bill and acceptance of using a personalized ad service that collects data. We find that willingness to use the app increases with the discount in three out of the four countries included.

When valuing personal data, it is common to focus on the value to the individual, and forget that data sharing has a positive external effect. The recommendation engine, for example of Amazon, is based on what all customers buy, and not only a single customer. Bergemann et al. (2022) call this social data. Data from one user could contain information that makes it easier to understand other users with a similar profile. The fact that data have this social dimension changes

the terms of trade between consumers, advertisers, and intermediaries like Facebook, since the external effect benefits the two latter actors. They conclude, however, that privacy regulations must take the external effect into account, and not just base the value of data on their value for the individual. The third paper in the thesis, on the use of data to combat a disease, partly shares the same logic, as the benefits of sharing personal data are realized at the societal, and not the individual level.

### **1.1.3 Personalization, marketing, and advertisements**

It is a standard point of view that marketing needs to be data-driven and, due to digitization, this has become easier according to Bleier et al. (2020). They use a contextual integrity framework to study how personalized marketing can trigger privacy concern. Based on contextual integrity, privacy is defined as *the right to an appropriate flow of personal information given the context*. This is different from the more common *the right to be left alone definition*, used by Warren and Brandeis (1890). The social context could be health care, education, or a marketplace, and norms and privacy concern will differ across contexts. They find that smaller firms might have a disadvantage compared to larger firms, and also that privacy concerns can foster innovation. According to Chen et al. (2019), Online Personalized Advertising (OPA) could make consumers perceive services as better than non-personalized ads would, but it could also give rise to unfavorable beliefs such as privacy concern. Striking a balance between concern and value is what marketeers have to master. They describe how concern would result in reactance to OPA, in this context meaning that consumers will click less on the ad. On the other hand, the perceived cost of not receiving OPA would lead to less reactance and more clicks. Kaaniche et al. (2020) show that so-called Privacy Enhancing Technologies (PETs) could facilitate personalization without being at the cost of privacy. In the second paper, we study a personalized ads service provided by a mobile operator, which sends ads via texts. Looking at the big picture, willingness decreases as the app demands more personal data and increases when a discount on the cell phone bill is introduced.

### **1.1.4 Regulation and consent**

The introduction of GDPR constituted a fundamental change in privacy regulations. The first paper in the thesis touches on the introduction of GDPR, and how it might have affected privacy concern and knowledge. The effects of its introduction have been studied by Godinho de

Matos and Adjerid (2022). Privacy consents became active and more detailed, and non-compliance would result in very high fines. The literature on the effects of regulation on data sharing is ambiguous. On the one hand, more detailed regulations could result in consumers sharing less data, while, on the other, the regulations could increase trust and reduce concern, and thereby increase willingness to share. They randomize customers of a telecoms provider into two groups and vary the point in time when they receive an email in which they are asked to consent under GDPR. The enhanced consent forms result in customers accepting more data usage after the introduction of GDPR than before. However, this does not apply to the most intrusive types of data (location and data being shared with third parties). The access to data makes the firm in question able to provide a better service, make more sales, and earn more money. The fourth paper studies consent decisions, and we find that ignorance, i.e. not seeking the privacy information, is rather common.

### **1.1.5 Privacy in health care and crises**

There is extensive literature on health care information and privacy. A better flow of information, facilitated by digital technology, could increase the quality of health care. At the same time, however, there is a growing need to protect personal data (Appari and Johnson, 2010). Adjerid et al. (2016) look specifically at privacy issues related to Health Information Exchange (HIE) in the US. These are systems where health information is shared across units in the U.S. health care system. They find that privacy regulation alone can have a negative impact on the development of HIEs, but that, combined with incentives, the regulations can have a positive impact.

Another interesting question is whether external shocks, like the COVID-19 pandemic, can fundamentally change the general state of digital privacy. Brough and Martin (2021) claim that privacy has suffered during the pandemic. First, there has been more public surveillance. In addition, activities that have normally been conducted physically, have now moved online, generating more data, e.g., meetings of Alcoholics Anonymous will now be held online and not physically. People who were pushed online during the pandemic could also lack knowledge about how to protect their data. Working from home could also mean working on less secure infrastructure, putting data at risk. They also claim that privacy rights, once lost, are rarely re-established. Their conclusion is that there is a need to strike a balance between appropriate crisis control and privacy rights.

The fact that people's lives are increasingly digital and that this, in turn, increases privacy

risks was an important motivation for the work on this thesis. There is no doubt that the pandemic has further accelerated this development and made digital privacy even more relevant. Paper number three in this thesis focuses on governments' use of personal data for disease control purposes, and it is relevant both to governmental surveillance and health economics.

### **1.1.6 Information economics**

Privacy in itself is about sharing personal information with others, or keeping it private, and Acquisti et al. (2016) categorize the economics of privacy as a sub-field of information economics. The economic literature on information provides insights into sub-fields other than the economics of privacy that are also relevant to this thesis. According to classical economic theory, privacy information will be beneficial. When making a decision, in this case when deciding whether or not to use a service, having more information would help individuals make better decisions (Stigler, 1961). Consumers should benefit from having as much information as possible, also about privacy and the use of personal data, when deciding what services to use. However, in certain situations, people decide to avoid information, even when the costs of accessing it are low. Sharot and Sunstein (2020), present a framework model for how people decide to seek or avoid information, when there is a trade-off between the positive and negative impact on people's welfare. In the fourth paper, avoidance of privacy information is the key element. In our third paper, we look at the role of information from a different angle. We conduct an experiment where participants are given different information about the consequences of sharing personal data, and then look for differences in behavior.

## **1.2 Data**

The papers constituting this thesis are all empirical. Three of them are based on survey data, while the fourth is based on an online experiment on the crowdsourcing platform Prolific Academic. Table 1 gives an overview of the papers. The starting point for the work and the data collection is somewhat unusual, since, throughout the process, it has been an integral part of the work of the Research and Innovation department of the multinational telecommunication provider Telenor. Examples of related work from Telenor R&I are Rosenthal et al. (2020), who study privacy awareness and trust in Facebook, and Evjemo et al. (2020), who provide an introduction



to privacy issues in relation to mobile communication. The use of personal data as a means of personalizing and improving service offerings has been part of the research agenda for a long time. On the other hand, understanding customers attitudes to such data usage, and their privacy preferences has also been an important topic. The data used in the first two papers are a direct result of the ambition to gain actionable business insight into the use of personal data.

The first two papers are based on data collected in 2017 among young users of mobile internet in countries where Telenor operates. The purpose of the surveys was to gain a better understanding of mobile internet use in the respective markets. The main privacy elements were measures of privacy awareness (privacy concern and privacy knowledge), and the level of actions the respondents take to protect their personal data and privacy. In spring 2018, both the Cambridge Analytica scandal and the introduction of GDPR in the EU took place. These events led to extensive media coverage of privacy issues in Norway, which motivated a re-run of the questions about awareness and protective actions in early summer 2018. The combination of the 2017 data from Norway and the second wave from 2018 constitutes the data used in Paper 1.

The Paper 2 data were collected across four countries: Malaysia, Norway, Pakistan, and Serbia, in the 2017 wave. The purpose was to gain a better understanding of mobile internet users' preferences as regards personalized services, and, more specifically, whether they were willing to give up their personal information to receive tailored advertisements through text messages from their cell phone operator. To get an idea of the valuation of personal data, it was relevant to examine the effect of a discount on respondents' cell phone bills. This was introduced for a randomized half of the sample in each country. In these cases, the description of the advertisement service included information that the user would get a ten percent discount. Introducing a monetary incentive in the form of a discount on cell phone bills also made it easier to compare very different countries.

During the outbreak of the COVID-19 pandemic, it soon became clear that data gathering by the health authorities through cell phones could become a controversial privacy topic, and this is the topic in Paper 3. Even though the data gathering was not conducted by the cell phone operator, their technology was at its core. For a cell phone operator, it seemed sensible to take steps to prepare for debates about the use of tools such as tracing apps. At the same time, a better understanding of people's attitudes to, e.g. tracing apps could potentially contribute to such tools becoming a success. These elements motivated us to launch a survey in April 2020 in Norway

and Sweden, a short time after the pandemic started in the two countries. Due to the fact that we, already at this stage, saw that Norway and Sweden were making very different political choices, it was interesting to compare the two countries. To monitor developments over time, we ran a second survey wave in late 2020.

The fourth paper is motivated by the large number of privacy choices the average consumer must make during their everyday digital lives. Very few, if any, are able to actually take in all privacy settings for all services they use, and we wanted to gain a better understanding of the choice between seeking out or avoiding information. We gathered data on such choices by conducting an online randomized experiment on Prolific, with participants from the US and Canada. The participants were presented with different videos from Telenor and had to make a privacy choice. We chose these countries because we did not want the participants to make their choices based on prior knowledge of Telenor.

### **1.3 Paper summaries**

In this section, we will summarize the four papers. Table 1 presents the objective, key content, theory, data, method and high level findings in the four papers for easy comparison. We then summarize each paper. The objectives of all the papers are variations on understanding privacy preferences or behavior. Three papers focus on the business-customer relationship, where the potential benefit of sharing personal data accrues to the individual. The last paper looks at a situation in which the health authorities collect data from individuals, while the positive effects benefit everyone. In one paper, the data are collected through the crowdsourcing platform Prolific, while surveys are used in the three others. The geographical footprint differs, and seven different countries on three different continents are covered, including countries that are outside what is referred to as the WEIRD (western, educated, industrialized, rich, and democratic) area.

Table 1: Overview of the papers

<b>text Paper 1: Digital Privacy — Knowledge, Concern and Behavior</b>					
<b>Objective</b>	<b>Key content</b>	<b>Theory</b>	<b>Data</b>	<b>Method</b>	<b>Findings</b>
To increase understanding of privacy from a customer perspective. To map personal characteristics and behavior, and identify changes after increased media coverage.	Measures of concern, knowledge and protective actions. Examining correlations between concern and knowledge and protective actions.	Privacy paradox: People claim to care about privacy but do not act accordingly. Conceptual framework: media coverage raises awareness and affects behavior.	A two-wave survey among young Norwegians in 2017 and 2018.	Surveys conducted before and after the Cambridge Analytica scandal and the introduction of GDPR, events that led to increased media coverage. Analyzed using OLS.	An increase in privacy knowledge and a small decrease in concern. No privacy paradox. Many participants take protective actions. These actions increase with high concern and high knowledge.
<b>Paper 2: Your privacy for a discount? Exploring willingness to share personal data in return for personalized offers</b>					
<b>Objective</b>	<b>Key content</b>	<b>Theory</b>	<b>Data</b>	<b>Method</b>	<b>Findings</b>
To explore young mobile internet users' acceptance of a personalized text message-based ad service provided by their cell phone provider. Explore privacy in non-WEIRD countries.	Studying the likelihood of using a personalized ad service based on location and browsing history. Identifying factors that may explain variations in this likelihood.	Literature suggests that people value their privacy and that the more personal data a service collects and uses, the less likely people are to use it.	Survey of young mobile Internet users in Malaysia, Norway, Pakistan, and Serbia in 2017.	RCT where half of the sample get a 10% discount on cell phone bills. Analyzed using ordered logit.	Use of service increases with a discount, except in Malaysia. Willingness decreases when more data are collected.
<b>Paper 3: Privacy during Pandemics: Attitudes to Public Use of Personal Data</b>					
<b>Objective</b>	<b>Key content</b>	<b>Theory</b>	<b>Data</b>	<b>Method</b>	<b>Findings</b>
To understand the willingness to share personal data when the benefit is at the societal level. Specifically, studying attitudes to sharing personal data with health authorities to combat a serious contagious disease.	Mapping attitudes to data-sharing for disease control purposes, testing the effect of information on health gains and privacy costs.	Literature predicts that information about potential gains will increase willingness to share data, while information on potential losses will decrease willingness to share data.	Two-wave survey data among the adult population in Norway and Sweden in April and November 2020.	RCT with 3 groups, one receiving information about benefits, one about costs, and a control group. OLS with Privacy Attitude Index as the dependent variable.	More information about benefits increases willingness to share data, while additional information about costs does not change attitudes. A clear purpose also increases willingness.
<b>Paper 4: Information Avoidance and Privacy — the Role of Entertaining Content</b>					
<b>Objective</b>	<b>Key content</b>	<b>Theory</b>	<b>Data</b>	<b>Method</b>	<b>Findings</b>
To better understand whether people seek out or avoid privacy information while online, and how different content might affect this choice.	Online experiment with varying levels of entertainment in content and the time cost of reading privacy information. Examine the decision to read or not read the privacy information.	Theory suggests that information can positively or negatively affect well-being, and that entertaining content can influence whether people choose to avoid or seek out information.	Online experiment conducted on Prolific Academic in May 2022. Participants from USA and Canada.	RCT with two groups, watching videos with different levels of entertainment and indicated reading time, using logit estimations to analyze the decision to read or not read privacy information.	Results indicate that a high time cost and a high level of entertainment could decrease the likelihood of reading privacy information. Further research is needed.

### **1.3.1 Paper 1: Digital Privacy - Knowledge, Concern, and Behavior (in Norwegian Digitalt personvern - kunnskap, bekymring og adferd)**

The aim of this article is to contribute to a better understanding of privacy from a customer perspective. Both knowledge of privacy regulations and an understanding of consumers' privacy limits will be key competences for businesses in the years ahead. Companies must comply with regulations, while at the same time striking a balance between customers' privacy needs and their demand for customized services. This is difficult and, for businesses, there are risks on both sides. Insufficient use of personal data may result in competitors providing better services and winning customers. If too much data are used, customers may feel that their privacy is invaded, and change supplier. In order to manage this two-sided risk, it is important to understand the customer's preferences and attitudes related to the use of personal data.

In summer 2017, we conducted a survey among young Norwegian consumers, aged 16-36, to study awareness of digital privacy, measured through two key concepts in the privacy literature: privacy concern (Kobsa et al., 2016; Westin, 2003) and privacy knowledge (Park, 2013; Trepte et al., 2015). We further looked at how this awareness influences privacy behavior. In spring 2018, the introduction of the EU's new privacy regulation and the Cambridge Analytica scandal received a lot of media attention. To see whether this resulted in changes in privacy awareness, we conducted a new survey in 2018.

We find that young adults in Norway are conscious about digital privacy. The level of concern is high. The level of knowledge is not as high, but it increased significantly from 2017 to 2018. A large proportion also take active steps to protect their data, and there is a positive correlation between both high concern and high knowledge, on the one hand, and protective actions, on the other. This is driven by the interaction, that is, by those who are both concerned and knowledgeable. The so-called privacy paradox (Kokolakis, 2017), that people say they are concerned but do nothing about it, finds little support in our data. Companies that plan to use personal data must understand and adapt to knowledgeable and concerned customers. Privacy and careful use of personal data can then become a competitive advantage, instead of a legal challenge.

### **1.3.2 Paper 2: Your privacy for a discount? Exploring willingness to share personal data in return for personalized offers**

This paper explores consumers' willingness to share personal data in return for receiving personalized offers on their cell phones. As the internet has become more widespread, the possibility of gathering personal data about consumers has increased, and our study is part of the growing literature on privacy preferences (Acquisti et al., 2015, 2020) and personalized ads and services (Tucker, 2014). Spiekermann et al. (2001) state that "Long existing dreams of one-to-one marketing are close to coming true . . .".

We ran survey experiments in nationwide surveys of mobile users, 16–35 years old, in Norway, Serbia, Malaysia, and Pakistan. We asked participants about the likelihood that they would use personalized text-based advertising services delivered through their mobile operator. We varied the level of personal data collected and whether it would be shared with third parties. In all four countries, the respondents' likelihood of using a personalized ad service decreases when the service used more personal data or when data were shared with third parties.

Using a randomized split-sample design, we found that introducing a 10 percent discount on cell phone subscriptions for those using the ad service increased the stated likelihood of using the service. Using this design, we find a comparable valuation of privacy across the geographies. In general, we find that the discount works, the respondents are able to make the trade-off and put a value on their personal data. We find significant differences in privacy attitudes between countries, with respondents in high-income Norway being least willing and those in low-income Pakistan most willing to share personal data. We identify only minor differences between respondents in Serbia and Malaysia, both middle-income countries.

The study contributes to the literature on the willingness to share personal data by including young adult respondents from countries in both Europe and Asia. By going beyond the typical WEIRD (western, educated, industrialized, rich, and democratic) samples used in most digital privacy studies (Acquisti et al., 2020), this article provides new insights from non-WEIRD countries and makes it possible to compare WEIRD and non-WEIRD countries. Furthermore, framing the survey questions in a mobile service context is appreciably closer to telecoms reality than most existing experimental studies on the sharing of personal data.

### 1.3.3 Paper 3: Privacy during Pandemics: Attitudes to Public Use of Personal Data

This paper studies the *privacy calculus* that people use to weigh the benefits of using a service or tool against the cost of disclosing their personal data (Dinev and Hart, 2006) in a non-commercial context. The public sector also launches online services that rely on data from citizens. One example of this is the health authorities' use of digital tools to combat COVID-19 (Budd et al., 2020). This included the use of digital contact-tracing apps, the gathering of cell phones' locations to understand mobility patterns, and targeted communication based on where people are. The use of personal data in this context was subject to much public debate, particularly with respect to civil rights and privacy (e.g., Kaya (2020); Sweeney (2020)). Some tracing apps have failed because of privacy issues, such as the first version of the Norwegian "Smittestopp" app.<sup>2</sup> Understanding people's attitudes to public use of personal data is therefore paramount if such tools from the health authorities are to be a success.

We investigate whether people are positive about sharing data with health authorities. We include the role personal characteristics might play in shaping these attitudes. We also test whether providing information about the costs and benefits of data usage have an effect on privacy attitudes. We collected survey responses from Norway and Sweden in spring and fall 2020. First, respondents answered questions about their personal characteristics that could affect privacy attitudes: their concerns about privacy, their knowledge about privacy, their general trust in several companies and public agencies, as well as their preferences as regards government interventions and individual self-sacrifice. We then measured our outcome variable, namely whether respondents had positive or negative attitudes to different types of data collection by the health authorities. These questions were asked after randomizing the respondents into three groups as part of a survey experiment. We assigned respondents to different versions of an introductory text, which emphasized either the cost or the benefit of personal data usage. A third group did not receive any additional information and was used as a control group.

We find that being concerned about privacy is negatively correlated with attitudes to public entities using personal data. On the other hand, high trust in entities collecting information and strong collectivist preferences are positively correlated. In addition, we do not find any significant relationship between privacy knowledge and privacy attitudes. Turning to the experiment,

---

<sup>2</sup><https://techcrunch.com/2020/06/15/norway-pulls-its-coronavirus-contacts-tracing-app-after-privacy-watchdogs-warning/>

we find that respondents receiving information about the public health gains are more positive to public use of personal data than those in the control group. We find no significant effect of providing additional information about the privacy costs. Given the large differences in the policies adopted to combat the pandemic in Norway and Sweden (Vogel, 2020), we found surprisingly few differences in citizens' attitudes to sharing data with the authorities.

#### **1.3.4 Paper 4: Information Avoidance and Privacy — the role of Entertaining Content**

In this study, we test whether someone exposed to highly entertaining online content is more likely to avoid privacy information than someone exposed to less entertaining content. According to classical economic theory, having more information will help individuals to make better decisions (Stigler, 1961). Sharot and Sunstein (2020), however, present a model for information avoidance where dis-utility as a result of a potential reduction in hedonic well-being could be a reason to avoid information. There is a well-established link in the literature between entertaining media content and hedonic well-being (Rieger et al., 2014). We study information avoidance in a specific privacy context. Privacy information could typically be an online company's privacy policy, what personal data are collected, and how the personal data will be handled, or a website's cookie settings.

In addition to investigating the role of entertaining content when a consumer decides whether to seek out privacy information or not, we also look at the time cost of seeking information. We ran an experiment online on the crowdsourcing platform Prolific Academic, with participants from the US and Canada. The participants were asked to watch and rate two videos produced by the multinational telecommunication provider Telenor. They were randomized into two groups, one group watching highly entertaining videos and the other group watching less entertaining, more informative videos. The participants were also randomly given different information about how much time it would take to access the privacy information before deciding whether or not to read a privacy notice. The key measurement in our experiment is whether or not participants decide to access the privacy information. In addition, we ask the respondents about their beliefs about how large a share of the other participants had been highly entertained when watching the first video. They had to base this belief on their own experience while watching the video, which

serves as an alternative measure of entertainment. We also measure the time the participants spend on the different steps throughout the experiment, making it possible to explore any variations in decision times across treatments. Privacy concern and trust, common measures from the privacy literature that might affect the behavior, are also included.

Our results show a tendency whereby participants exposed to more entertaining content and a higher reading time are less likely to read the privacy notice. When testing the two treatments, we find significantly fewer readers among those exposed to long reading time, but no effect for the content treatment. However, when substituting the content treatment with secondary beliefs about entertainment levels, we partly find a significantly lower share of readers for higher levels of entertainment as well. The participants were asked whether they expected their user experience to be affected by the privacy information. The share expecting a negative impact was larger among those in the entertaining treatment group. Furthermore, looking at how much time the participants spent on deciding whether to read the privacy information, we find that it was significantly shorter among those who watched entertaining videos. Our findings indicate that the type of content and time cost could play a role when people have to choose whether to access or avoid privacy information, but more research is needed to fully understand this potential relationship.

## **1.4 Concluding remarks**

The objective of the thesis was to gain a better understanding of privacy preferences and behavior, and how personal data are shared in digital everyday life. First, I would claim that people do care about privacy. In the thesis, this topic is illuminated from very different angles. One extreme is the commercial personalized advertising service where the benefit of sharing personal data is reaped by the individual, and another is how personal data can be used to combat an infectious disease with the benefits being reaped on the collective level. The data material in the various articles was collected in countries that are very different in terms of both their technological and economic development, and in relation to attitudes to privacy and its status in law. Europe has a set of strict regulations in place, and similar legislation exists in individual states in the US, while, elsewhere, laws are far less extensive and sometimes close to non-existent. Despite these differences, there are some similarities that recur in all four articles. Firstly, we see that a large proportion of respondents are concerned about their privacy when using digital services. Further-



more, it is clear that high levels of concern are accompanied by a lower willingness to share data. Trust in the actor who collects data, whether a mobile operator or the health authorities, is also a recurring factor. If an actor who wants to use personal data in its activities enjoys a high degree of trust, it will make the users or customers who are encouraged to share their data more benevolent.

In many contexts, users of digital data-driven services must make a trade-off between sharing their personal data and gaining benefits from using the service. This must be done without a market price or other clear, easily accessible information that can help the users to make their choices. However, we see from our findings that our respondents are generally weighing up the costs and disadvantages. We find that transparency about why data are collected and what they will be used for can increase willingness to share, one possible reason for which is that the choice simply becomes easier. Furthermore, we find that receiving financial compensation for sharing one's data increases one's willingness to do so. Our findings indicate that the individual's privacy has common features with a normal economic good.

At the same time, the choices are very complicated, and the entity that collects data will often be the strongest party, and I agree with Acquisti et al. (2020) that this is a very complicated and difficult choice for an ordinary user. Their recommendation is that users must be given protection through strict regulations, and I agree with that. This is largely already in place in Europe, but it is important for *regulatory authorities* to remember that the fact that information must be made available does not mean that it will actually be read and understood. Regulations can still be developed to make information more easily accessible to users. Furthermore, measures, preferably in schools, to increase knowledge about how data are used, and potentially misused, will make it easier for individuals to make their own choices. Knowledge will also make it easier to handle privacy concerns.

For *companies* that use personal data in their business, we will repeat the recommendations from Paper 1. Companies must understand their customers' privacy preferences and adapt to concerned and knowledgeable customers. Furthermore, companies should be clear about their intentions, which, in turn, can contribute to increased trust. Companies that succeed in delivering the services customers want, without being invasive, will be in a position to gain an advantage in the market.

The thesis has contributed to new knowledge about people's preferences and behavior related to the use of personal data in several areas. However, more research is also needed in the

areas covered in this thesis and many more. For example, there is something that is still unresolved in the results relating to entertaining content and information avoidance, where more work is needed. I would emphasise the area where the gap is perhaps biggest: gaining more knowledge from outside the WEIRD demographic, where I especially hope to see a lot of research in the future.

To sum up, I give Mark Twain's words the following slight tweak: *The reports of the death of privacy are greatly exaggerated.*

## References

- Acquisti, A., L. Brandimarte, and G. Loewenstein (2015). Privacy and human behavior in the age of information. *Science* 347(6221), 509–514.
- Acquisti, A., L. Brandimarte, and G. Loewenstein (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology* 30(4), 736–758.
- Acquisti, A., L. K. John, and G. Loewenstein (2013). What is privacy worth? *The Journal of Legal Studies* 42(2), 249–274.
- Acquisti, A., C. Taylor, and L. Wagman (2016). The economics of privacy. *Journal of economic Literature* 54(2), 442–92.
- Adjerid, I., A. Acquisti, and G. Loewenstein (2019). Choice architecture, framing, and cascaded privacy choices. *Management Science* 65(5), 2267–2290.
- Adjerid, I., A. Acquisti, R. Telang, R. Padman, and J. Adler-Milstein (2016). The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science* 62(4), 1042–1063.
- Amnesty International (2019). Surveillance giants: How the business model of google and facebook threatens human rights.
- Appari, A. and M. E. Johnson (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management* 6(4), 279–314.
- Athey, S., C. Catalini, and C. Tucker (2017). The digital privacy paradox: Small money, small costs, small talk. Technical report, National Bureau of Economic Research.

- Bergemann, D., A. Bonatti, and T. Gan (2022). The economics of social data. *The RAND Journal of Economics* 53(2), 263–296.
- Bleier, A., A. Goldfarb, and C. Tucker (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing* 37(3), 466–480.
- Brough, A. R. and K. D. Martin (2021). Consumer privacy during (and after) the covid-19 pandemic. *Journal of Public Policy & Marketing* 40(1), 108–110.
- Budd, J., B. S. Miller, E. M. Manning, V. Lampos, M. Zhuang, M. Edelstein, G. Rees, V. C. Emery, M. M. Stevens, N. Keegan, et al. (2020). Digital technologies in the public-health response to covid-19. *Nature medicine* 26(8), 1183–1192.
- Chen, Q., Y. Feng, L. Liu, and X. Tian (2019). Understanding consumers' reactance of online personalized advertising: A new scheme of rational choice from a perspective of negative effects. *International Journal of Information Management* 44, 53–64.
- Council of Europe (1950). Convention for the protection of human rights and fundamental freedoms. *as amended by Protocols Nos. 11 and 14, 4 November*.
- Dienlin, T. and J. Breuer (2022). Privacy is dead, long live privacy! two diverging perspectives on current issues related to privacy. *Journal of Media Psychology: Theories, Methods, and Applications*, Advance online publication. <https://doi.org/10.1027/1864-1105/a000357>.
- Diggelmann, O. and M. N. Cleis (2014). How the right to privacy became a human right. *Human Rights Law Review* 14(3), 441–458.
- Dinev, T. and P. Hart (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research* 17(1), 61–80.
- Evjemo, B., G. Grønnevet, R. Ling, W. Nag, H. L. Røhr, and O. C. Wasenden (2020). Privacy on Smartphones: A Cross-National Study. In *The Oxford Handbook of Mobile Communication and Society*. Oxford University Press.
- Godinho de Matos, M. and I. Adjerid (2022). Consumer consent and firm targeting after gdpr: The case of a large telecom provider. *Management Science* 68(5), 3330–3378.

- Kaaniche, N., M. Laurent, and S. Belguith (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications* 171, 102807.
- Kaya, E. K. (2020). Safety and privacy in the time of covid-19: Contact tracing applications.
- Kobsa, A., H. Cho, and B. P. Knijnenburg (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An elaboration likelihood model approach. *Journal of the Association for Information Science and Technology* 67(11), 2587–2606.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64, 122–134.
- Kummer, M. and P. Schulte (2019). When private information settles the bill: Money and privacy in google’s market for smartphone applications. *Management Science* 65(8), 3470–3494.
- Lyon, D. (2014). Surveillance, snowden, and big data: Capacities, consequences, critique. *Big data & society* 1(2), 2053951714541861.
- Marreiros, H., M. Tonin, M. Vlassopoulos, and M. Schraefel (2017). Now that you mention it”: A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization* 140, 1–17.
- Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication research* 40(2), 215–236.
- Rieger, D., L. Reinecke, L. Frischlich, and G. Bente (2014). Media entertainment and well-being—linking hedonic and eudaimonic entertainment experience to media-induced recovery and vitality. *Journal of Communication* 64(3), 456–478.
- Rosenthal, S., O. C. Wasenden, G.-A. Grønnevet, and R. Ling (2020). A tripartite model of trust in facebook: acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology* 23(6), 840–864.
- Savage, S. J. and D. M. Waldman (2015). Privacy tradeoffs in smartphone applications. *Economics Letters* 137, 171–175.

- Sharot, T. and C. R. Sunstein (2020). How people decide what they want to know. *Nature Human Behaviour*, 1–6.
- Spiekermann, S., J. Grossklags, and B. Berendt (2001). E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pp. 38–47.
- Stigler, G. J. (1961). The economics of information. *Journal of Political Economy* 69(3), 213–225.
- Svirsky, D. (2022). Privacy and information avoidance: An experiment on data-sharing preferences. *The Journal of Legal Studies* 51(1), 63–92.
- Sweeney, Y. (2020). Tracking the debate on covid-19 surveillance tools. *Nature Machine Intelligence* 2(6), 301–304.
- Trepte, S., D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind (2015). Do people know about privacy and data protection strategies? towards the “online privacy literacy scale”(oplis). In *Reforming European data protection law*, pp. 333–365. Springer.
- Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of marketing research* 51(5), 546–562.
- United Nations (1948). Universal declaration of human rights. *General Assembly Resolution 217A III) of*.
- Vogel, G. (2020). Sweden’s gamble. *Science* 370(6513), 159–163.
- Warren, S. D. and L. D. Brandeis (1890). The right to privacy. *Harvard Law Review*, 193–220.
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues* 59(2), 431–453.
- Whitman, J. Q. (2003). The two western cultures of privacy: Dignity versus liberty. *Yale LJ* 113, 1151.
- Winegar, A. G. and C. R. Sunstein (2019). How much is data privacy worth? a preliminary investigation. *Journal of Consumer Policy* 42(3), 425–440.

# Paper 1





# Digitalt personvern – kunnskap, bekymring og adferd <sup>F</sup>



**OLE CHRISTIAN WASENDEN** er samfunnsøkonom fra UiO. Han jobber i Telenors forskningsavdeling, primært med konkurransestrategi og kundeforståelse. I 2018 ble han også tilknyttet Handelshøyskolen ved NMBU som nærings-ph.d. med digitalt personvern som forskningstema.

## SAMMENDRAG

Mengden av persondata som genereres gjennom bruk av digitale tjenester, er stadig økende. Målet med denne artikkelen er å bidra til en bedre forståelse av personvern fra et kundeperspektiv. Både kunnskap om personvernregelverk og forståelse av forbrukernes personverngrenser vil være nøkkelkompetanse for næringslivet i årene som kommer. Bedrifter må trå rett i forhold til regelverk og samtidig finne en balanse mellom kundenes personvernbehov og deres ønsker om tilpassede tjenester.

Sommern 2017 gjennomførte vi en spørreundersøkelse blant unge norske forbrukere for å studere bevissthet om digitalt personvern, målt gjennom bekymrings- og kunnskapsnivå. Vi så videre på hvordan denne bevisstheten påvirket personvernadferd. Våren 2018 fikk

innføringen av EUs nye personvernregulering og den såkalte Cambridge Analytica-skandalen mye omtale i mediene. For å se om dette ga endringer i personvernbevissthet, gjennomførte vi en ny undersøkelse i 2018.

Vi finner at unge voksne har et bevisst forhold til digitalt personvern. Bekymringsnivået er høyt. Kunnskapsnivået er ikke like høyt, men økte betydelig fra 2017 til 2018. En stor andel tar også aktive grep for å beskytte dataene sine. Det såkalte personvernparadokset – at brukere er bekymret, men ikke gjør noe med det – får lite støtte i våre data.

Bedrifter som skal bruke persondata, må forstå og tilpasse seg de kunnskapsrike og bekymrede kundene. Da kan personvern og varsom bruk av personlige data bli et konkurransefortrinn, i stedet for en juridisk utfordring.

## INTRODUKSJON

Mange bedrifter bruker persondata i tjenesteutvikling og kundepleie, og vil gjerne levere personaliserte tjenester som er like bra som Amazons bokanbefalinger. Disse er ofte relevante, og man forstår hvorfor de dukker opp, og hvilke data som er brukt. Kunder verdsetter at personlig informasjon brukes til å skape

gode og effektive tjenester, men databruken bør ikke bli for nærgående. Hvis en bedrift trår over grensen til det private, kan det ha negative konsekvenser for kundenes tillit. Å balansere hensynene mellom tilpassede tjenester og personvern er vanskelig, og for næringslivet finnes det risiko på begge sider. For lite bruk av personlige data kan resultere i at konkurrenter

leverer bedre tjenester og vinner kundene. Brukes for mye data, kan kundene oppleve at privatlivet invaderes, og de bytter leverandør. For å håndtere denne tilsidige risikoen er det viktig å forstå kundens preferanser og holdninger knyttet til bruk av personlige data. Målet med denne artikkelen er å bidra med innsikt om unge norske forbrukere samt presentere et analytisk rammeverk og konkrete eksempler fra Norge.

Med smarttelefoner og raske mobile datanettverk har personvernproblematikk gått inn i ny æra. Privat-sfæren innsnevres når telefonen er full av apper som logger aktivitet. Intensjonen er ofte god, og informasjonen brukes til å utvikle gode produkter og tjenester. Samtidig utgjør dette en potensiell trussel mot personvernet, og brukerne er bekymret for at data kan komme på avveie og misbrukes. Det er hevdet at vi står overfor et personvernparadoks, der forbrukere er bekymret, men ikke gjør noe for å passe på dataene sine (Kokolakis, 2017).

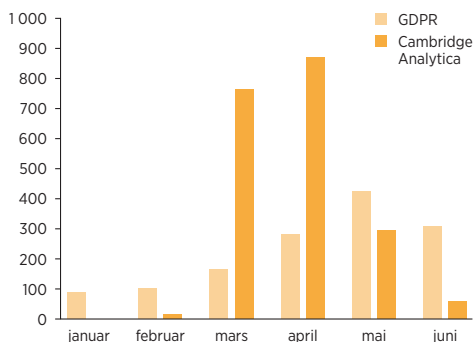
Våren 2018 fikk to personvernsaker bred dekning i norske medier (se figur 1): den såkalte Cambridge Analytica-skandalen og innføringen av EUs nye personvernregulering (General Data Protection Regulation, GDPR). Mediedekningen belyste to sentrale temaer knyttet til hvordan persondata brukes i digitale markeder: Cambridge Analytica-oppslagene viste hvordan data kan misbrukes, mens GDPR-oppslagene viste hvordan nytt regelverk skal hindre slikt.

Kjernen i Cambridge Analytica-skandalen var at Facebook-data fra rundt 87 millioner mennesker, hovedsakelig i USA, ble brukt til politisk påvirkning uten at de var klar over det (Isaak & Hanna, 2018; Tjøstheim & Høibø, 2019). Cambridge Analytica brukte innsamlende data til formål de ikke hadde kommunisert. Selskapet høstet også data fra brukere de ikke hadde kontakt med. Dataene ble brukt til å predikere personlighet, altså informasjon som mange vil oppleve som svært personlig. Skandalen resulterte blant annet i et krav om strengere regulering i USA (Isaak & Hanna, 2018).

Ny regulering på personvernområdet ble innført i EU og Norge i mai 2018. Reguleringen, kjent som GDPR, er ment å styrke EU-borgernes personvernrettigheter og privatliv når samfunnet blir stadig mer datadrevet. For en nærmere gjennomgang av GDPR, se for eksempel Jarbekk og Sommerfeldt (2019).

Gjennom denne artikkelen vil vi bidra til en bedre forståelse av personvern fra et kundeperspektiv. Opp-

FIGUR 1 Antall oppslag i norske medier våren 2018 om GDPR og Cambridge Analytica. Kilde: Retriever



trer unge nordmenn i tråd med personvernparadokset? Har kundene et bevisst og aktivt forhold til digitalt personvern? Hvordan kan en som næringsaktør tilnærme seg problemstillingen? Økt kunnskap om kundenes forhold til personvern vil sette bedrifter bedre i stand til å gjøre gode valg knyttet til utnyttelse av kundedata.

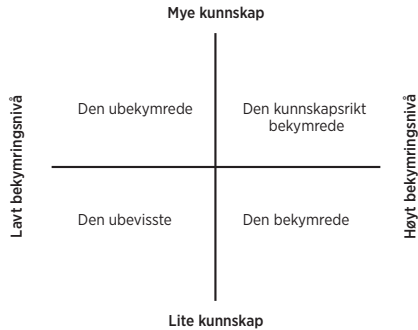
## LITTERATURGJENNOMGANG

Litteraturen på personvern er rik, og vi vil her kort dekke tre ulike undertema som er viktige for vår studie: (1) personvernbevissthet, målt ved bekymrings- og kunnskapsnivå, (2) adferd, både knyttet til deling av data og å beskytte egne data, og (3) det såkalte personvernparadokset. En oversikt over hvordan personlige data brukes kommersielt i utvalgte bransjer i Norge, finnes i Dulsrud og Alfnes (2017).

### PERSONVERNBEVISSTHET

I mange studier brukes bekymringsnivå som eneste mål på personvernbevissthet. Basert på bekymringsnivå deles forbrukerne ofte inn i *fundamentalister*, *pragmatikere* og *ubekymrede*. Denne segmenteringen ble introdusert av Alan Westin i 1995 (Westin, 2003). Westin har gjennomført en rekke personvernundersøkelser helt tilbake til 1978, og indekserer og studert utvikling av blant annet bekymringsnivå. Kumaragura og Cranor (2005) gir en systematisk gjennomgang av Westins arbeid. Kobsa, Cho og Knijnenburg (2016)

FIGUR 2 Bevissthetsmatrise for personvern.



videreutvikler målingen av personvernbehandling i en digital kontekst.

Kunnskapsnivå er et viktig komplement til bekymring. Park (2011) deler personvernkunnskap i tre deler: kunnskap om tekniske sider ved internett, kunnskap om hvordan internetselskaper samler og bruker personlig informasjon, og kunnskap om politikktutforming knyttet til personvern. Park og Jang (2014) tar også med hva forbrukerne aktivt er i stand til å gjøre for å beskytte dataene sine. Trepte og medforfattere (2015) legger til kunnskap om personvernrisiko og -trusler og hvordan slike trusler bør håndteres.

I Evjemo og medforfattere<sup>1</sup> (2020) kombineres kunnskaps- og bekymringsnivå i en bevissthetsmatrise for personvern, se figur 2. Der deles forbrukerne inn i segmentene *den ubevisste*, *den bekymrede*, *den bekymringsløse* og *den kunnskapsrikt bekymrede*. Bekymring måles gjennom seks påstander, i hovedsak basert på Kobsa og medforfattere (2016). Kunnskap måles gjennom ni kunnskapsspørsmål, delvis basert på Trepte og medforfattere (2015) og Park og Jang (2014). Vi bruker bevissthetsmatrisen i vår analyse og kommer tilbake til dette i metod delen.

Flere studier ser også på hvilke drivkrefter som former personvernbevissthet. En mye brukt parameter er

<sup>1</sup> I arbeidet til Evjemo og medforfattere (2020) brukes det samme 2017-datasettet som vi bruker i denne studien. De studerte effekter på tvers av land, mens vi gjør dypere analyser av Norge og ser på endringer fra 2017 til 2018.

hvordan en bedrift presenterer sine personverninnstillinger (se for eksempel Tsai mfl., 2011). Vi kjenner ikke til arbeid som undersøker effekter av medieoppdrag på personvernbevissthet. Sammenhengen mellom mediedekning, kunnskap og adferd er imidlertid veletablert i for eksempel politisk økonomi. I Prat og Strömberg (2013) beskrives hvordan mediedekning og mediekonsum øker innsikt i politiske saker, og hvordan dette igjen påvirker stemmeadferd.

#### ADFERD

Tidligere empiriske studier av temaer som er sentrale for vårt arbeid, gjennomgås i en oversiktsartikkel av Acquisti, Brandimarte og Loewenstein (2015). De oppsummerer eksisterende forskning langs tre dimensjoner. Den første er usikkerhet knyttet til konsekvensene av å dele data. Det er uklart for forbrukerne hva dataene brukes til, og vanskelig å sette en verdi på mulige negative konsekvenser. For det andre er oppfattelsen av hvor grensen mellom det private og det offentlige går, kontekststavnghengig. For det tredje er faktorene som påvirker bekymringsnivå og adferd knyttet til personvern, manipulerbare. For eksempel kan ulike utforminger av en webside gjøre at et spørsmål besvares ulikt (John, Acquisti, & Loewenstein, 2011). Mange forbrukere har lite kunnskap om disse temaene, mens en kommersiell aktør ofte har inngående kunnskap om hvordan de kan stimulere til datadeling.

Et eksperiment gjennomført blant tyske brukere av en internettside (Utz mfl., 2019) viser hvor lett adferd kan påvirkes. Deltagerne i eksperimentet ble gitt forskjellige varianter av et banner for å akseptere informasjonskapsler, eller såkalte *cookies*. Enkel bruk av såkalt dulting (eng. *nudging*) (Thaler & Sunstein, 2009), der utformingen dulter brukeren i en bestemt retning, hadde tydelig utslag på adferd. For eksempel økte akseptandelen fra 39,2 til 50,8 prosent når aksepterknappen gikk fra å være grå til å være tydelig framhevet. En studie av effekter på norske forbrukere etter innføring av GDPR finnes i Berg og Dulsrud (2018).

Wills og Zeljkovic (2011) studerer spesifikke handlinger for å beskytte egne data, som sletting av informasjonskapsler, bruk av privat nettlesingsmodus og sletting av nettleserhistorikk. Spørsmål om denne typen handlinger brukes også i undersøkelser av kunnskapsnivå. En norsk studie av Brandtzaeg, Pultier og Moen (2019) finner at over halvparten av responden-

tene har latt være å laste ned eller bruke en app mer enn én gang, fordi den krever tilgang til informasjon brukeren ikke vil dele.

#### PERSONVERNPARADOKSET

Begrepet personvernparadokset knyttet til deling av personlige data på internett ble introdusert tidlig på 2000-tallet. Barnes (2006) bruker personvernparadokset som betegnelse på det at ungdom deler informasjon om seg selv på sosiale nettverk, og deretter blir overrasket over at foreldrene deres leser det. Begrepet brukes imidlertid annerledes i dag, og paradokset ligger i at brukere av digitale tjenester har et høyt bekymringsnivå knyttet til personvern, men gjør lite med det. Athey, Catalini og Tucker (2017) viser at bekymrede forbrukere er villige til å dele personlige data mot en lav betaling. En litteraturgjennomgang av Kokolakis (2017) finner at det ikke er noen konsensus om personvernparadoksets eksistens.

#### RAMMEVERK OG HYPOTESER

Sommeren 2017 gjennomførte Telenor Research en spørreundersøkelse blant unge voksne i Norge. Undersøkelsen fokuserte på sammenhengen mellom personvernbevissthet og adferd myntet på å beskytte personlige data. Våren 2018 fikk personvernsspørsmål høy mediedekning gjennom Cambridge Analytica-skandalen og innføringen av GDPR. Dette åpnet muligheten for å se etter endringer og var bakgrunnen for at en ny undersøkelse ble gjennomført i 2018.

Basert på eksisterende litteratur har vi satt opp rammeverket gjengitt i figur 3. Mediedekning av personvernrelaterte spørsmål vil kunne påvirke personvernbevissthet. Her har vi hentet inspirasjon fra politisk økonomi. Videre vil personvernbevissthet ha betydning for adferd, og denne sammenhengen er relativt bredt beskrevet i litteraturen. Studier av personvernparadokset ser spesielt på sammenhengen mellom bekymring og adferd.

Våre data gir et begrenset grunnlag for å finne en årsakssammenheng mellom mediedekning og personvernbevissthet. Vi observerte personvernbevissthet før og etter medieomtalen, men har ingen kontrollgruppe eller randomisering. I tillegg til tidsrekkefølgen på observasjonene og medieomtalen vil vi støtte oss på tidligere litteratur. Den peker i retning av at mye mediedekning om et tema resulterer i økt kunnskap i befolkningen (se Prat & Strömberg, 2013). Antatt sammenheng mellom mediedekning og bekymringsnivå er litt mer komplisert og vil trolig avhenge av innholdet i mediedekningen. Cambridge Analytica-omtalen vil trolig virke negativt på bekymringsnivået, men GDPR-omtalen trolig positivt. Vi formulerer derfor ikke hypoteser for det første steget i rammeverket, men vil drøfte utviklingen i personvernbevissthet fra 2017 til 2018 med bakgrunn i den økte mediedekningen.

For det andre steget i rammeverket formulerer vi tre forskningshypoteser som ser på sammenhengen mellom bevissthet og adferd, og på personvernparadokset:

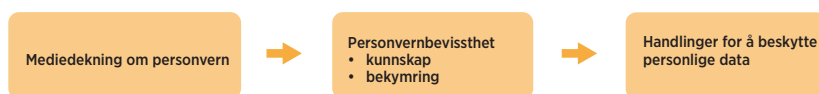
- H1: Bekymring for digitalt personvern er positivt korrelert med aktivitet for å beskytte sine personlige data.
- H2: Kunnskapsnivå om personvern er positivt korrelert med aktivitet for å beskytte sine personlige data.
- H3: Unge voksne gjør aktive handlinger for å beskytte sine personlige data.

#### METODE

##### UTVALG OG SPØRREUNDERSØKELSER

Basert på spørreundersøkelser fra 2017 og 2018 ser vi på norske forbrukere i aldersgruppen 16 til 35 år. Datainnsamlingen ble i begge tilfeller gjennomført av Kantar TNS på oppdrag av Telenor Research. Respondentene i begge undersøkelsene er trukket fra Kantars webpanel, med mål om å få sammenlignbare utvalg. 2017-utvalget har 838 respondenter, og 2018-utvalget har 505.

FIGUR 3 Konseptuelt rammeverk for sammenhenger mellom mediedekning, bevissthet og handlinger.



TABELL 1 Sammenligning av demografi i 2017- og 2018-utvalget.

DEMOGRAFI	2017 (N = 838)	2018 (N = 505)
Alder		
16–20	12,29 %	16,63 %
21–25	24,58 %	28,71 %
26–30	37,59 %	26,73 %
31–35	25,54 %	27,92 %
Kjønn		
Kvinner	46,78 %	61,98 %
Menn	53,22 %	38,02 %

Note: sammenligning alder  $\chi^2(1) = 1,38; p = 0,24$ , sammenligning kjønnsfordeling  $\chi^2(1) = 1,38; p = 0,00$

Tabell 1 gir en oversikt over alder og kjønn i de to utvalgene. En ikke-parametrisisk Kruskal-Wallis-test viser ingen signifikante forskjeller i alderssammensetningen. En kjkvadrattest viser signifikante forskjeller i kjønnsfordelingen mellom de to undersøkelsene, med en overvekt av kvinner i 2018-utvalget. I analysene vil vi derfor kontrollere for kjønn.

#### INDEKSER FOR BEKYMRINGS- OG KUNNSKAPSNIVÅ

Målingen av personvernbekymring og -kunnskap er basert på Evjemo og medforfattere (2020). Tabell 2 viser de fem utsagnene som brukes til å måle personvernbekymring.<sup>2</sup> Respondentene svarte på i hvor stor grad de var enige i utsagnene på en femdel Likert-skala fra «svært enig» til «svært uenig». Vi tilordner hver respondent en indeksskår basert på svarene på de fem spørsmålene.<sup>3</sup> Når vi summerer opp svarene, gir de fem svarkategoriene en skår fra minus to for svært ubekymret, til to for svært bekymret. Vi kategoriserer en respondent som «bekymret» hvis hun får en samlet skår på to eller høyere.

Kunnskapsindeksen er basert på ni påstander som enten er sanne eller usanne. Påstandene er gjengitt i tabell 3.<sup>4</sup> Respondentene ble også her gitt fem svaralternativ fra «helt sikkert sant» til «helt sikkert usant». Når vi summerer opp svarene, gis de minus to hvis de

2 Utsagnene har en Cronbachs alfa på 0,84, som indikerer at de i stor grad måler det samme underliggende konsept.

3 Vi har valgt å utelate et utsagn, til tross for at det ble brukt av Evjemo og medforfattere, fordi påstanden ikke er entydig.

4 Utsagnene har en Cronbachs alfa på 0,75, som indikerer at de i akseptabel grad måler det samme underliggende konsept.

TABELL 2 Utsagn knyttet til bekymring.

UTSAGN BENYTTET TIL BEKYMRINGSINDEKSEN
Jeg er bekymret for at internettbaserte selskap samler inn for mye personlig informasjon om meg
Det plager meg at jeg ikke kan kontrollere hvordan min personlige informasjon blir brukt av internettbaserte selskaper
Det plager meg vanligvis når mobil-apper spør meg om personlig informasjon
Jeg tror at mobil-apper spør om mer personlig informasjon enn det som trengs til formålet med appen
Det plager meg at personlig informasjon gitt til et internettbasert selskap for et spesielt formål, kan brukes til andre formål

TABELL 3 Kunnskapspåstander.

KUNNSKAPSPÅSTANDER
Facebook, Google og lignende selskaper følger din aktivitet på internett
Mange mobilapper registrerer din lokasjon
Sosiale nettverksoperatører som for eksempel Facebook samler inn informasjon også om dem som ikke bruker Facebook
Når en mobil-app har en personvernerklæring, betyr det at personlige data ikke blir delt med andre apper eller selskaper
Facebook, Google og lignende selskaper sletter personlige data etter en forhåndsbestemt periode
De som lager apper, samler kun inn det av personlig informasjon som er nødvendig for at tjenesten skal fungere
Når du deaktiverer GPS på din mobiltelefon, kan ikke din lokasjon spores
Din nettleserhistorikk vil normalt lagres på mobiltelefonen din
Det er ikke mulig å hacke privat informasjon fra din mobiltelefon

har svart «helt sikkert sant» og utsagnet er usant. Tilsvarende gis de to hvis de har svart «helt sikkert sant» og utsagnet er sant. Som hos Evjemo og medforfattere kategoriserer vi en respondent som kunnskapsrik hvis hun får en samlet skår på ni eller høyere.

For å se på personverrelaterte handlinger spurte vi respondentene om de aktivt beskytter sine personlige data. Eksempler på slike handlinger er å slette *cookies* og å slå av lokasjonsfunksjonen på mobiltelefonen. Vi spurte om seks handlinger, og respondentene fikk alternativene «oftere enn en gang i måneden», «sjeldnere enn en gang i måneden», «aldri, fordi jeg ikke ser noe behov» og «aldri, jeg vet ikke hvordan det gjøres».

TABELL 4 Regresjoner – endringer i kunnskaps- og bekymringsnivå.

	(1) KUNNSKAPSNIVÅ	(2) KUNNSKAPSNIVÅ	(3) BEKYMRINGSNIVÅ	(4) BEKYMRINGSNIVÅ
ÅR	0,735* (0,291)	1,067*** (0,285)	-0,578** (0,213)	-0,562** (0,214)
ALDER		0,139*** (0,028)		0,091*** (0,021)
KVINNE		-1,869*** (0,283)		0,071 (0,212)
KONSTANT	-1 455,9* (586,3)	-2 128,5*** (574,8)	1 170,6** (429,1)	1 135,7** (431,0)
N	1 343	1 343	1 319	1 319
ADJ. R <sup>2</sup>	0,004	0,063	0,005	0,018

Standardfeil i parentes, \* $p < 0,05$ , \*\* $p < 0,01$ , \*\*\* $p < 0,001$

Dette gir oss mulighet til å se hvorvidt respondentene er bekymret og passive, altså handler i tråd med det såkalte personvernparadokset, eller om de aktivt tar grep for å bedre sitt personvern.

## RESULTATER

Våre funn støtter opp om de tre forskningshypotesene, og vi kan forkaste de tilhørende null-hypotesene om at 1) bekymring for digitalt personvern ikke er positivt korrelert med aktivitet for å beskytte sine personlige data, 2) kunnskapsnivå om personvern ikke er positivt korrelert med aktivitet for å beskytte sine personlige data, og 3) unge voksne ikke gjør aktive handlinger for å beskytte sine personlige data. Våre resultater viser også en betydelig økning i personvernkunnskap, og en reduksjon i personvernbekymring, i løpet av omtrent et halvt år. Vi kan ikke konkludere sikkert med at det skyldes mediedekning, men vi finner det sannsynlig at dette er årsaken. Hvilke faktorer som påvirker personvernbevissthet, er et tema det bør forskes videre på.

### ENDRINGER I KUNNSKAPS- OG BEKYMRINGSNIVÅ FRA 2017 TIL 2018

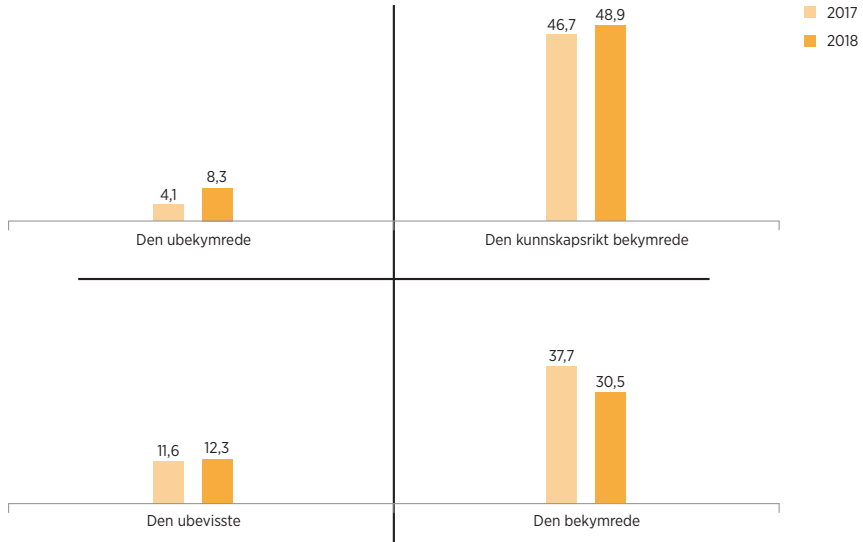
Nordmenn har et aktivt forhold til digitalt personvern. Bekymringsnivået, målt med vår indeks, var høyt både i 2017 og 2018, med nivåer på henholdsvis cirka 84 og 79 prosent. Vi ser altså en nedgang, og dette er likt for begge kjønn. Andelen med et høyt kunnskapsnivå i 2017 var

42 prosent for kvinner og 58 prosent for menn. Disse økte til henholdsvis 48 og 72 prosent i 2018, altså en økning for begge kjønn, men nivåene er høyere for menn.

Tabell 4 viser resultater fra to ulike regresjoner for henholdsvis kunnskaps- og bekymringsnivå hvor vi ser nærmere på endringene som har skjedd fra 2017 til 2018, og kontrollerer for kjønn og alder. I den første regresjonen ser vi bare på effekten av tidsparameteren, mens vi i den andre kontrollerer for kjønn og alder. Både økningen i kunnskap og reduksjonen i bekymringsnivå fra 2017 til 2018 er signifikante, også når vi kontrollerer for kjønn og alder. Videre ser vi at innenfor denne aldersgruppen, 16 til 35 år, øker både kunnskap og bekymring om digitalt personvern signifikant med alder. Kvinner har signifikant lavere digital personvernkunnskap enn menn.

Figur 4 illustrer hvordan respondentene fordeler seg på de fire segmentene i bevissthetsmatrisen til Evjemo og medforfattere (2020) i henholdsvis 2017 og 2018. Andelen *kunnskapsrikt* er høyere i 2018 enn 2017, og økningen fordeler seg både på *de ubekymrede* og *de kunnskapsrikt bekymrede*. Gruppen som tidligere kun var bekymret, er mest redusert fra 2017- til 2018-undersøkelsen. Det er verdt å merke seg at segmentet med *de kunnskapsrikt bekymrede* er den klart største gruppen. Vi kommer tilbake til betydningen av dette når vi nå skal se nærmere på sammenhengen mellom personvernbevissthet og handlinger for å beskytte dataene sine.

FIGUR 4 Bevissthetsmatrisen – endringer i de ulike segmentene fra 2017 til 2018.



TABELL 5 Prosentandeler som gjør handlingen mer enn én gang i måneden, aldersgruppe 16–35, 2017 og 2018. N = 1 343.

	TOTALT	DEN UBEVISSTE	DEN BEKYMREDE	DEN UBEKYMREDE	DEN KUNNSKAPSRIKT BEKYMREDE
Slette nettleserhistorikk	24,8	19,2	23,7	17,1	28,1
Benytte privat-/inkognitofane ved nettsurfing	40,1	26,6	29,7	51,3	49,6
Blokkere cookies/informasjonskapsler	21,1	9,7	15,1	18,4	28,6
Slå av lokasjonsfunksjonen for å ikke spores	33,2	18,7	32,6	11,8	39,8
Bruke nettleserversjonen av en tjeneste i stedet for appen	26,4	13,9	21,5	20,0	33,6
Avbryte installasjonen av en app fordi du blir spurt om å oppgi for mange personlige data	18,8	9,6	17,6	4,0	23,6

Note: sammenslåtte data fra både 2017 og 2018

#### BESKYTTELSE AV EGNE DATA

Det store flertallet unge voksne bruker ett eller flere virkemidler for å beskytte dataene sine. Totalt i begge våre undersøkelser er det bare 5 prosent som ikke gjør noe. I tabell 5 ser vi for eksempel at 40 prosent i denne alder-

gruppen bruker en privat fane når de surfer, minst én gang i måneden. 33 prosent skruer av lokasjon like hyppig.

Basert på de seks mulige handlingene beregner vi et totalt aktivtetsnivå som ligger på mellom 0 og 12. Når vi summerer opp handlingene, gis en skår på to

TABELL 6 Regresjon – totalt handlingsnivå for enkeltrespondenter på tvers av år som avhengig variabel.

	(1) AKTIVITETSNIVÅ	(2) AKTIVITETSNIVÅ	(3) AKTIVITETSNIVÅ	(4) AKTIVITETSNIVÅ
KUNNSKAPSNIVÅ	0,101*** (0,016)		0,087*** (0,016)	0,034 (0,025)
BEKYMRINGSNIVÅ	0,238*** (0,0210)		0,238*** (0,021)	-0,0500 (0,103)
KVINNE		-0,881*** (0,163)	-0,756*** (0,154)	-0,735*** (0,154)
ALDER		0,042** (0,016)	0,009 (0,015)	0,008 (0,015)
ÅR		-0,263 (0,164)	-0,208 (0,155)	-0,187 (0,155)
INTERAKSJON KUNNSKAP OG BEKYMRING				0,0109** (0,004)
KONSTANT	1,577*** (0,398)	4,899*** (0,461)	2,187*** (0,559)	3,510*** (0,725)
<i>N</i>	1 319	1 343	1 319	1 319
ADJ. <i>R</i> <sup>2</sup>	0,158	0,034	0,176	0,181

Standardfeil i parentes, \**p* < 0,05, \*\**p* < 0,01, \*\*\**p* < 0,001

hvis de gjør en handling oftere enn én gang i måneden, en skår på én hvis de gjør den sjeldnere enn én gang i måneden, og null hvis de ikke gjør den aktuelle digitale personvernhandlingen.

For å se på sammenhengen mellom personvernhandlinger og kunnskap og bekymring presenterer vi i tabell 6 fire regresjoner som alle benytter data fra både 2017 og 2018. Den avhengige variabelen er det totale aktivitetsnivået. Modell 1 har kun kunnskap og bekymring som forklaringsvariabler, og vi finner at begge er signifikant positive. Både økende kunnskap og økende bekymring gir høyere aktivitetsnivå. Modell 2 har kjønn, alder og år som forklaringsvariabler, og vi finner at kjønn er signifikant. Kvinner gjør færre personvern tiltak. Resultatene fra modell 1 og 2 holder fortsatt når vi i modell 3 slår sammen de to første. Vi finner en positiv effekt fra bekymring og kunnskap, og at kvinner har et lavere aktivitetsnivå enn menn, gitt samme kunnskap og bekymringsnivå. Når vi i modell 4 tar med en interaksjonseffekt mellom kunnskap og bekymring, ser vi at det kun er denne interaksjonsef-

fekten, i tillegg til effekten av kjønn, som er signifikant. Dette vil si at hvis man både har høyt kunnskapsnivå og høyt bekymringsnivå, gir det høyt nivå på handlinger for å beskytte data. De enkelte komponentene, kunnskap og bekymring, er ikke lenger signifikante.

Med andre ord er det de nesten 50 prosentene som befinner seg i *kunnskapsrikt bekymrede*-segmentet, oppe til høyre i bevissthetsmatrisen, som virkelig skiller seg ut fra de andre når det gjelder å beskytte dataene sine.

## DISKUSJON OG OPPSUMMERING

I samfunnsdebatten har en kunnet høre utsagn som at «privacy is dead». Dette er for eksempel budskapet i en artikkel i Forbes (Morgan, 2014) med overskriften «Privacy is completely and utterly dead, and we killed it». Hovedpoenget i Forbes-artikkelen var at vi omgir oss med så mange tjenester som samler inn og lagrer data, at det er umulig å opprettholde et digitalt privatliv. Dette er selvsagt en forenkling, men påstanden danner et godt bakteppe for å diskutere våre funn.



Hvis personvernet er dødt, skulle man tro at flertallet av dagens unge voksne ikke bryr seg, noe som rimer dårlig med våre funn.

I vår analyse har vi studert flere aspekter ved norske unge voksne sitt forhold til deling av persondata i en digital kontekst. Det er vanskelig å unngå at ens personlige data samles og brukes av en rekke aktører, i tråd med «personvern er dødt»-påstanden. Våre analyser peker imidlertid i retning av at bevissthetsnivået er høyt. En svært stor andel svarer at de er bekymret for hvordan data brukes, og over halvparten av gruppen som undersøkes, har et høyt kunnskapsnivå. Vi finner også at mange tar aktive grep for å beskytte dataene sine.

#### ENDRES PERSONVERNBEVISSTHET I EN PERIODE MED HØY MEDIEDEKNING?

Fra 2017 til 2018 økte andelen kunnskapsrike fra 42 til 48 prosent for kvinner og fra 58 til 72 prosent for menn. I løpet av denne relativt korte perioden på litt over et halvt år vet vi at mediedekningen av personvernsprosjekt var stor. Som beskrevet har vi ikke gjennomført noe kontrollert eksperiment for å studere effekten av mediedekningen på personvernbevisstheten. Basert på forskning på slike effekter fra andre forskningsfelt forventet vi imidlertid et økt kunnskapsnivå. Våre funn er i tråd med denne forventningen.

Bekymringsnivået er høyt både i 2017 og 2018. Det var nærliggende å tro at Cambridge Analytica-skandalen skulle resultere i en ytterligere økning i bekymring, men resultatene viser at nivået gikk noe ned. En mulig grunn kan være innføringen av GDPR. Når det blir innført ny og strengere regulering mynnet på å bidra til at kundedata ikke skal kunne misbrukes, vil det kunne redusere bekymringsnivået. Økt kunnskapsnivå kan også gi redusert bekymringsnivå. Det er mulig at forbrukerne har fått nok kunnskap til å oppleve at de har kontroll.

#### AKTIVE HANDLINGER OG PERSONVERNPARADOKSET

Våre analyser indikerer at mange unge voksne tar aktive grep for å beskytte dataene sine. Imidlertid ser vi at det er forskjeller mellom de ulike typene i bevissthetsmåtrisen, og at det er *de kunnskapsrike bekymrede* som gjør mest. Denne gruppen er den klart største både i 2017 og 2018.

Samtidig som forbrukerne er bekymret for sine personlige data, bruker et stort flertall datagrådige tjenester som Facebook og Google. Dette gjelder også de som har høyt kunnskapsnivå, og som bruker forskjellige metoder for å beskytte dataene sine. Det er sannsynlig at brukerne veier nytte mot kostnad og bruker tjenester som oppleves som svært verdifulle, til tross for at de er datagrådige. Tjenester som har lavere nytteverdi, blir kuttet ut av hensyn til personvernet.

Det er vanskelig for brukere å forutse mulige framtidige konsekvenser av at data blir samlet i dag. Derfor er det vanskelig å veie mulige framtidige kostnader opp mot nytteverdien, som gjerne kommer umiddelbart. Dette er et av hovedtemaene som Acquisti og medforfatter (2015) diskuterer i sin oversiktsartikkel.

Vi finner ingen klar støtte for personvernparadokset i vår analyse og mener at konseptet i enkelte sammenhenger blir brukt på en måte som tar vekk nødvendige nyanser fra analysene. Vi mener framtidig forskning bør fokusere mer direkte på beslutningsprosessen for brukere går gjennom når de bestemmer seg for om de skal bruke en datagrådige tjeneste eller ikke. En bedre forståelse av denne beslutningsprosessen er etter vår mening viktigere enn å forstå selve personvernparadokset.

#### IMPLIKASJONER FOR BEDRIFTER OG MYNDIGHETER

Svært mange er bekymret for hvordan deres personlige data brukes. Samtidig er vårt utvalg splittet når det gjelder kunnskap. Dette bør det tas hensyn til når politikk skal utformes og framtidige kommersielle strategier utmeisles.

Digitaliseringen vil fortsette, og det vil også innsamling og bruk av personlige data. For at alle skal kunne delta og ha maksimalt utbytte av teknologien, bør mulige tiltak for å øke kunnskapsnivået og redusere bekymringsnivået løftes høyere opp på den politiske dagsorden.

For bedrifter kan kunders holdninger til personvern danne basis for et konkurransefortrinn. GDPR krever at kunder skal gi et opplyst samtykke før persondata kan brukes, og bedrifter har dette som en absolutt grense for hva som kan gjøres med persondata. Det er imidlertid mulig at forbrukere har andre smertepunkter enn de grensene som ligger i regelverket. Derfor må bedrifter forstå sine kunders personvernpreferanser og tilpasse seg bekymrede og kunnskapsrike kunder.

Bedrifter som lykkes med å levere de tjenestene kundene ønsker, uten å være invaderende, vil kunne få et fortrinn i markedet.

I sum vil vi konkludere med at personvernet ikke er dødt. En rekke medier har i januar 2020 meldt at Facebook gjør det lettere for sine brukere

å styre hvilke data selskapet skal bruke. Dette er ett av mange eksempler på at personvern tas på alvor. Med våre funn, som tydelig viser at personvern er noe mange er opptatt av, lurer vi på om vi i tiden framover vil se flere overskrifter i retning av «Privacy strikes back».

M

## REFERANSER

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015, 30. januar). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.
- Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: Small money, small Costs, small Talk. *NBER Working Paper*, 23488.
- Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 11–15.
- Berg, L., & Dulstrud, A. (2018). *Tillit og sårbarhet på nett. Forbrukernes praksiser og vurderinger etter innføringen av den nye personvernforordningen (GDPR) i Norge 2018* (SIFO oppdragsrapport nr. 9). Oslo: OsloMet.
- Brandtzaeg, P.B., Pultier, A., & Moen, G.M. (2019). Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. *Social Science Computer Review*, 37(4), 466–488.
- Dulstrud, A., & Alfnes, F. (2017). *Når stortada blir Big Business* (SIFO oppdragsrapport nr. 10). Oslo: OsloMet.
- Evjemo, B., Grønnevet, G. Ling, R., Nag, W., Røhr, H.L., & Wasenden, O.C. (2020). Privacy on smartphones: A cross-national study. I R. Ling, L. Fortunati, S.S. Lim, G. Goggin, & Y. Li (red.), *The Oxford handbook of mobile communication, culture, and information*. Oxford: Oxford University Press.
- Isaak, J., & Hanna, M.J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51(8), 56–59.
- Jarbekk, E., & Sommerfeldt, S. (2019). *Personvern og GDPR i praksis*. Oslo: Gyldendal Damm Akademisk.
- John, L.K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, 37(5), 858–873.
- Kobsa, A., Cho, H., & Knijnenburg, B.P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors. An elaboration likelihood model approach. *Journal of the Association for Information Science and Technology*, 67(11), 2587–2606.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134.
- Kumaragura, P., & Cranor, L.F. (2005). *Privacy indexes: A Survey of Westin's Studies* (Working paper CMU-ISRI-05-138). Carnegie Mellon University.
- Morgan, J. (19.08.2014). Privacy is completely and utterly dead, and we killed it. *Forbes*. Hentet 21.02.2020 fra <https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/>
- Park, Y.J. (2011). Digital literacy and privacy behavior online. *Communication Research*, 40(2), 215–236.
- Park, Y.J., & Jang, S.M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, 38, 296–303.
- Prat, A., & Strömberg, D. (2013). The political economy of mass media. *Advances in economics and econometrics*, 2, 135.
- Thaler, R.H., & Sunstein, C.R. (2009). *Nudge: Improving decisions about health, wealth and happiness*. London: Penguin Books.
- Tjøstheim, I., & Høibø, M. (2019). Nordmenn og deling av persondata (rapport nr. 1044). Oslo: Norsk Regnesentral.
- Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fisher, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the «Online Privacy Literacy Scale» (OPLIS). I S. Gutwirth, R. Leenes, & P. de Hert (Red.), *Reforming European data protection law* (s. 333–365). Heidelberg, Tyskland: Springer.
- Tsai, J.Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254–268.
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un) informed consent: Studying GDPR consent notices in the field. *Proceedings of the 2019 ACM Conference on Computer and Communications Security*. ACM Press, New York, USA.
- Westin, A.F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431–453.
- Wills, C., & Zeljkovic, M. (2011). A personalized approach to web privacy: Awareness, attitudes and actions. *Information Management & Computer Security*, 19(1), s. 53–73.

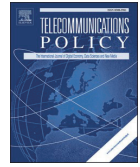
## **Paper 2**





Contents lists available at ScienceDirect

## Telecommunications Policy

journal homepage: [www.elsevier.com/locate/telpol](http://www.elsevier.com/locate/telpol)

# Your privacy for a discount? Exploring the willingness to share personal data for personalized offers<sup>1</sup>

Frode Alfnæs<sup>a,c</sup>, Ole Christian Wasenden<sup>a,b,\*</sup>

<sup>a</sup> School of Economics and Business, Norwegian University of Life Sciences, Norway

<sup>b</sup> Telenor Research, Norway

<sup>c</sup> Consumption Research Norway, Oslo Metropolitan University, Norway

## ARTICLE INFO

## JEL classification:

C83  
D82  
D83  
M37

## Keywords:

Personal data  
Preference elicitation  
Data privacy  
Mobile (cell) phone services

## ABSTRACT

This paper explores how willing consumers are to share personal data to receive personalized offers on their mobile (cell in the US) phones using nationwide surveys of mobile users, 16–35 years old, in Norway, Serbia, Malaysia, and Pakistan. We ask respondents about the likelihood they would use three types of personalized advertising services delivered through their mobile operator, with services varying with respect to the level of personal data collected and whether shared with third parties. In all four countries, respondents state that their likelihood of using a personalized ad service decreases when the service uses more personal data or shares the data with third parties. Using a split sample design, we find that introducing a 10% discount on mobile subscriptions for those using the ad service increases the stated likelihood of using the service. We find significant differences in willingness to share personal data attitudes between countries, with respondents in high-income Norway being least willing and those in low-income Pakistan most willing to share personal data. We identify only minor differences between respondents in Serbia and Malaysia, middle-income countries in Europe and Asia. The study contributes to the literature on the willingness to share personal data by including young adult respondents from countries in both Europe and Asia. Furthermore, framing the survey questions in a mobile service context is appreciably closer to telecom reality than most existing experimental studies on sharing of personal data.

## 1. Introduction

Imagine you are out shopping and a message lands on your mobile (cell in the US) phone. It contains an offer from a nearby store, tailored to match your interests. How do you feel? Today's technologies make it possible to combine knowledge of consumer preferences and detailed location data to target nearby potential customers with personalized offers on their mobile devices. However, consumers must give up some of their privacy and share personal data with commercial actors to receive such personalized offers. To explore the privacy-personalization tradeoff in a telecom setting, this paper investigates factors affecting mobile users' interest in mobile services using location data and browsing history to create personalized offers. We utilize survey data from a large telecommunications firm with business units in Europe and Asia. We study the privacy preferences of mobile users in Norway, Serbia,

<sup>1</sup> This research was supported by a grant from the Research Council of Norway.

\* Corresponding author. School of Economics and Business, Norwegian University of Life Sciences, Norway.

E-mail address: [olwa@nmbu.no](mailto:olwa@nmbu.no) (O.C. Wasenden).

<https://doi.org/10.1016/j.telpol.2022.102308>

Received 9 July 2021; Received in revised form 11 January 2022; Accepted 15 January 2022

Available online 7 February 2022

0308-5961/© 2022 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Malaysia, and Pakistan and investigate the country differences in the stated willingness to share location and browsing history with commercial actors to receive personalized offers.

The increasing use of smartphones and mobile Internet connections has significantly improved the possibility of collecting and using location and personal information from mobile users worldwide. Many online companies are part of the personal data ecosystem, and data on users are essential to their business (Chaudhry et al., 2015). These companies often operate in two-sided markets, selling data or ads space to advertisers and services and products to end-users (Acquisti et al., 2016). Google's Chief Economist Hal Varian (2010, 2014) describes the benefits of this development along four dimensions: more efficient data extraction and analysis, possibilities for personalization and customization of goods and services, easier to conduct experiments, and new kinds of contracts due to better monitoring.

The large amounts of data that online companies harvest result in a growing concern about privacy. Zuboff (2015) comments on Varian's benefits and states that they depend on an implicit logic of surveillance. Acquisti et al. (2020) argue that even when users of digital services take many steps to protect their privacy, they will unlikely attain desired levels. In response to these challenges, several countries have implemented laws and regulations to give citizens better control over their data, e.g., the European Union's General Data Protection Regulation and Japan's Act on the Protection of Personal Information (Schwartz, 2019). Among academics, we have seen a growing literature on consumer privacy preferences (Acquisti et al., 2015, 2020) and personalized ads and services (e.g., Segijn et al., 2021; Strycharz et al., 2019; Tucker, 2014).

A much-studied question in privacy research is whether consumers place a positive value on privacy and personal data. Related to this is the so-called privacy paradox that states that people claim they worry about digital privacy but do not act on their worries. A literature review by Kokolakis (2017) on the privacy paradox suggests mixed results. Some studies find that most consumers are unwilling to pay for privacy (e.g., Beresford et al., 2012), while others find that most consumers place some positive value on their privacy (e.g., Benndorf & Normann, 2018). In a recent review of the privacy literature, Acquisti et al. (2020) argue that ample evidence exists that people are both concerned about their privacy and take actions to protect it, even though it is not evident in all circumstances.

Acquisti et al. (2020) point out that most of the research on privacy is done in WEIRD (Western, Educated, Industrialized, Rich, and Democratic) countries. The usage of digital services that collect large amounts of personal data and the potential challenge that follows are not limited to the WEIRD countries. For example, the share of the population using Facebook are as high in several non-WEIRD countries as typically seen in WEIRD countries. According to NapoleonCat,<sup>1</sup> close to 86 percent of the population in Malaysia used Facebook in 2021, while the number for Norway, the WEIRD country in our study was 75 percent. Similar numbers for the two other non-WEIRD countries in our study are 52 percent in Serbia and 24 percent in Pakistan. To help reduce the knowledge gap of privacy preferences in non-WEIRD countries, we compare privacy attitudes in three non-WEIRD countries, Malaysia, Pakistan, and Serbia, with attitudes in Norway, a WEIRD country.

Several studies have investigated scale and scope sensitivity in privacy preferences regarding the amount of data the participants shared (scale effects) and how many they share it with (scope effects). For example, Benndorf and Normann (2018) elicit reservation prices for various bundles of personal data. They identify significant scope sensitivity when they ask participants to share contact and preference data, but not when they ask them to share different bundles of Facebook data. Schudy and Utikal (2017) find that German students' willingness to share personal data with anonymous recipients decreases with the number of recipients. However, they discover no scale effect arising from the amount of data each unknown recipient receives. These mixed results suggest the need for more research into scale and scope sensitivity in privacy preferences.

As the Internet became more widespread, the possibility of gathering personal data about consumers increased, and marketing academics started to investigate its effect on marketing practices. Several studies pointed to an expected increase in the use of personalization. Peppers et al. (1999) describe how a business could increase the value of its customer base through one-to-one marketing. Companies should change their marketing strategies and base them on what they know about the individual customer. Spiekermann et al. (2001) state that "Long existing dreams of one-to-one marketing are close to coming true...". O'Malley et al. (1997) discuss businesses using personal data in their market activities and conclude that what marketers call "intimacy" consumers could see as "intrusion". Hence, the literature on the balancing act of delivering good, personalized services and ads without invading the consumers' privacy is more than two decades in the making.

It is now possible for online ads to be personalized and tailored to specific users at specific times and in particular locations (Chen & Hsieh, 2012). The tailoring can make ads more relevant for the receiver (De Keyser et al., 2015). However, depending on how well the ads meet consumer preferences, they could be entertaining, informative or even irritating (Haghirian et al., 2008). Reviewing the current state and future of advertising research, Taylor and Carlson (2021) conclude that the advertising field has recently seen dramatic changes from technology advancements and new media consumption patterns. Increased understanding of the impact of these changes and further developments, including developments in privacy issues, still need more research.

Privacy concerns, privacy knowledge, and trust are often included in studies of online privacy behavior (Acquisti et al., 2016, 2020; Baruh et al., 2017; Evjemo et al.<sup>2</sup> 2020). We also use these attitudes and define them as done in the privacy and trust literature. Taylor et al. (2009) define privacy concern as a customer's concern for controlling the acquisition and subsequent use of information generated or acquired in online transactions. Trepte et al. (2015) split privacy knowledge into declarative knowledge - to understand risks and rights - and procedural knowledge - to understand how to protect personal data. In our study, we focus on declarative

<sup>1</sup> <https://napoleoncat.com>.

<sup>2</sup> Evjemo et al. (2020) explore the knowledge and concern measures used in this paper.

knowledge. Rosenthal et al. (2020) discuss trust in a digital setting and follow the definition of Mayer et al. (1995). They define trust as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer et al., 1995, p. 712). All three factors play a role in forming peoples’ privacy attitudes and behavior, and they are relevant as control variables in our study (Baruh et al., 2017; Brown & Muchira, 2004; Chellappa & Sin, 2005; Wang et al., 2016; Youn, 2009).

To shed light on consumers’ privacy behavior and valuation of privacy in non-WEIRD countries, we ran a survey experiment of young mobile Internet users in Serbia, Malaysia, and Pakistan and compared them to young mobile Internet users in Norway. As part of the survey experiment, we presented three versions of a personalized ad service and asked respondents to express their likelihood of using this service in a hypothetical scenario. The core of the service was that users will receive up to 10 ads a month via text messages that are personalized based on information the user chooses to share. We showed respondents three different variations of the ad service. The most basic version of the service only used location data. The next version of the service combined the location data with the browsing history. Notably, only the mobile operator receives the data for both the first and second service versions. The last version of the service combined location and browsing history and shared the information with the mobile operator and a third-party store. For half the participants, we described the ad services as including a 10% discount on their mobile subscription.

We identify scale and scope sensitivity regarding the amount of data shared and how many receive the data. While the stated likelihood of participants using the personalized ad service decreases when the mobile operator requests more personal data or shares the data with a third party, introducing a 10% discount on the mobile subscription for those using the ad service increases the likelihood of using the service. We identify significant effects of concern, knowledge, and trust on the respondents’ willingness to use the services. Comparing results across countries, we reveal substantial differences in these stated attitudes, with respondents in Norway being least willing and those in Pakistan most willing to share personal data, adding a geographical aspect to the heterogeneity of consumers.

## 2. Method

The privacy questions were included in a survey exploring mobile Internet usage conducted by a large European telecommunication firm in countries where they had business units in 2017. The surveyed countries were Norway, Serbia, Malaysia, and Pakistan, and the data collection was conducted by Kantar TNS, a leading global market research agency. Here, we describe the survey design, sample, and behavioral predictions related to privacy.

### 2.1. Design of survey experiment

The privacy survey experiment uses a split-sample design and three hypothetical survey questions. We ask respondents about how likely it is that they will use different services with specific characteristics using the question: “Consider the following service. How likely is it that you would use such a service?” with responses on a five-point scale (very likely, likely, neutral, unlikely, very unlikely).

We use a  $3 \times 2$  experimental design with a mix of within- and between-sample treatments. The experiment includes three levels of data sharing and two levels of discount, zero and 10%. The data-sharing factor is a within-sample factor where the respondents see all three levels, starting with the level where least data is shared. The discount factor is a between-sample factor, where we randomly draw respondents into one of the two treatments. In addition to these two experimental design factors, the four countries are between-sample factors.

The data-sharing factor is operationalized through services where the respondents receive a personalized offer from stores they pass or visit. The offer is either sent from their mobile operator or a third party. The core of the service is the tracking of user location, used by the mobile operator to send relevant offers. In the first service, the offers are only based on location. In the second service, the offers are based on location and interest, and in addition to location, the mobile operator must gather browsing history. The third service is identical to the second with respect to the data collected. However, in the third service, the data is shared with the stores the consumer visits, and the stores can send them offers. Table 1 presents the two factors used in the design, data sharing, and discount. We presented the respondents with one data-sharing service at a time (the within factor), all with either a discount or not (the between factor).

### 2.2. Samples and control variables

The respondents were drawn from online survey panels in Norway, Serbia, and Malaysia, while in Pakistan a combination of phone and face-to-face interviews were used. The sample was limited to 16–35-year-olds that use the Internet on their mobile phones.<sup>3</sup> Table 2 presents the sample demographics for the total sample and the four-country subsamples. We observe a skewness toward the older half of surveyed age span, with just 40% of respondents being between 16 and 25 years old. This skewness is especially prominent in Norway and Malaysia. Similarly, Serbia and Malaysia have a skewed gender balance, with more women responding than men. Accordingly, we include Gender and Age as control variables in our estimations to reduce the potential effects arising from the skewed samples on the outcome variable.

As described in the introduction, privacy concerns, privacy knowledge, and trust in mobile operators are frequently included in

<sup>3</sup> For this age group in Norway, Serbia, and Malaysia, the population shares using the Internet on their mobile are more than 90%; in Pakistan, 35% (Telenor internal data).

**Table 1**  
Factors in the design: Data sharing and discounts.

Factor and Level	Description
Factor 1: Data sharing	A within-sample factor with three levels
Service 1: Share location with the mobile operator	Consider a situation where you can receive offers via SMS from stores when you pass or visit them. The offers will be sent from your mobile operator. To receive this service, you must let your mobile operator track your current location. The mobile operator will not share your location data with any third parties. The number of SMSs is limited to 10 a month.
Service 2: Share location and browsing history with the mobile operator	Consider a situation where you can receive offers tailored to your interest via SMS from stores when you pass or visit them. The offers will be sent from your mobile operator. To receive this service, you must let your mobile operator track your current location and your Internet browsing history. The mobile operator will not share your location and browsing data with any third parties. The number of SMSs is limited to 10 a month.
Service 3: Share location and browsing history with the mobile operator, which then shares it with a third party	Consider a situation where regardless of where you are, you can receive offers tailored to your interest via SMS from stores you visit often. The offers will be sent from the relevant stores. To receive this service, you must let your mobile operator track your location history and your Internet browsing history and <i>share</i> it with the stores you visit. The number of SMSs is limited to 10 a month.
Factor 2: Discount	A between-sample factor with two levels
0% discount	You receive no discount on your mobile service
10% discount	You receive a 10% discount on your mobile service

**Table 2**  
Sample demographics and background attitudes on privacy and trust.

Demographics	Total		Norway		Serbia		Malaysia		Pakistan	
	N	%	N	%	N	%	N	%	N	%
Sample	3244		838		777		856		782	
Male	1442	44.5	446	53.2	267	34.5	340	40.0	389	49.7
Female	1802	55.5	392	46.8	506	65.5	511	60.0	393	50.3
Age										
16–20 years	528	16.3	103	12.3	141	18.3	90	10.6	194	24.8
21–25 years	751	23.2	206	24.6	152	38.0	193	19.7	200	25.6
26–30 years	1051	32.5	315	37.6	262	34.0	282	33.3	192	24.6
31–35 years	980	28.0	214	25.5	216	28.0	282	33.3	196	25.0
Standardized attitudes	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.
Trust in mobile operator	0.00	1.00	0.04	0.96	-0.17	0.98	-0.41	0.86	0.56	0.93
Privacy concern	0.00	1.00	0.11	1.04	0.22	0.98	-0.13	0.91	-0.20	1.00
Privacy knowledge	0.00	1.00	0.80	0.94	0.22	0.96	-0.36	0.76	-0.68	0.59

studies of consumer behavior. Because these factors could affect the willingness of consumers to use a personalized ad service, we include them in our analysis as controls. We standardize these three variables to have a mean of zero and a standard deviation of one using the total sample.

The lower panel of Table 2 presents the means and standard deviations for these three variables for each country. Positive mean values for trust, concern, and knowledge indicate that for that country, the respondents have greater trust in their mobile operators, more concern about privacy, and better knowledge about privacy than the average respondent in the four-country sample. As shown, there are considerable differences between respondents in the four countries sampled, especially concerning privacy knowledge, which is much higher in Norway, slightly higher in Serbia and lower in Malaysia and Pakistan. For more details on these measures, see the appendix.

Table 3 presents balance tests for the randomization into price discount treatment groups in each of the four countries. The treatment variable is a categorical variable with two levels. We employ a Kruskal–Wallis equality-of-populations rank test for Age, with p-values ranging from 0.10 to 0.65, and a Chi-square test for Gender with p-values ranging from 0.10 to 0.74. Gender is a categorical variable with two levels, while Age is an interval variable that is close to uniformly distributed with no tails. The test results indicate that the demographic variables are well balanced across the two treatments in all four countries.

### 2.3. Behavioral predictions

There is extensive economic literature on sharing personal information, but according to Acquisti et al. (2016), it is challenging to locate a unifying economic theory of privacy. Consequently, we base our behavioral predictions on the assumptions that (1) consumers value privacy, (2) consumers are willing to make tradeoffs between privacy and money, (3) privacy is a continuous measure (i.e., privacy comes in degrees, and not only have or have not), and (4) the number of actors receiving the information affects the level of



**Table 3**  
Balance test for the variables Age and Gender to confirm randomization.

Country	Variable	Mean with discount	Mean without discount	p-value <sup>b</sup>
Norway	Age	27.10	26.51	0.10
Norway	Gender <sup>a</sup>	1.44	1.50	0.10
Serbia	Age	26.53	26.66	0.65
Serbia	Gender	1.63	1.68	0.15
Malaysia	Age	28.00	27.80	0.49
Malaysia	Gender	1.59	1.61	0.74
Pakistan	Age	25.96	25.73	0.58
Pakistan	Gender	1.53	1.47	0.15

<sup>a</sup> Male = 1, Female = 2.

<sup>b</sup> Kruskal–Wallis equality-of-populations rank test for Age and Chi-square test for Gender.

privacy.

Our experiment allows us to study stated preferences along three dimensions of privacy: (1) the amount of personal data shared – the scale effect, (2) resharing of personal data with other commercial actors – the scope effect, and (3) economic incentives to share personal data. For these three dimensions, we formulate three behavioral predictions.

### 2.3.1. The amount of personal data shared

Assuming that privacy has a value to consumers and is not dichotomous, we expect consumers to prefer to share as little as possible about themselves with commercial actors: we expect a negative scale effect on the willingness to share. We formulate the following hypothesis:

**Hypothesis 1.** The willingness of consumers to share personal data will decrease when asked to share browsing history along with the location.

### 2.3.2. Resharing personal data with other commercial actors

Assuming that the number of recipients of personal data affects consumer privacy, we expect consumers to prefer to share their data with as few others as possible: we expect a negative scope effect on the willingness to share. We formulate the following hypothesis:

**Hypothesis 2.** The willingness of consumers to share personal data will decrease when asked to share data with retailers in addition to the mobile operator.

### 2.3.3. Economic incentives

Assuming that consumers are willing to trade privacy for money, we expect consumers to be more inclined to share personal data if they are economically compensated. In our case, the benefit is relevant offers, while for half the sample, an extra economic benefit arises from the 10% discount on the mobile subscription. We formulate the following hypothesis:

**Hypothesis 3.** The willingness of consumers to share personal data will increase if the sharing is connected to a discount on the mobile subscription.

## 2.4. Cross-country variation

Along with the three dimensions in the behavioral predictions, we also include cross-country dimensions. The four countries (Norway, Serbia, Malaysia, and Pakistan) differ in many economic and social respects, as illustrated by the United Nations' Human Development Index and the Telecommunication Infrastructure Index. For the United Nations' Human Development Index, the four countries range from the top to the lowest quartile. For example, in 2017 Norway ranked 1 of 189 countries included in the index, Malaysia ranked 57, Serbia ranked 67, and Pakistan ranked 150 (United Nations Development Program, 2018). A similar picture emerges with the Telecommunication Infrastructure Index (United Nations, 2020), which combines mobile and fixed subscriptions and Internet usage. Here, Norway scored 0.90, Malaysia 0.76, Serbia 0.62, and Pakistan 0.24 on a scale from 1 to 0. However, as these are country-level variables, we do not use them in our statistical analysis. Instead, these differences represent an essential background when discussing the differences between the countries in our findings.

## 3. Results

This section presents the mean scores for responses to the likelihood of use questions and the estimation results for the likelihood of use of the services when regressed against discounts, demographics, and attitudes as independent variables. We also evaluate the three behavioral predictions and explore any differences by country.

### 3.1. The average likelihood of using the ad services

Fig. 1 depicts the average likelihood of using the ad service requiring personal data. We can see a pattern where the participants, on average, are most favorable to Service 1, which only requires sharing location data with the mobile operator. They are slightly less favorable to Service 2, which requires sharing both location data and browsing history with the mobile operator, and least favorable to Service 3, which requires the sharing location history and the browsing history with both the mobile operator and a third party. We can also see that the participants offered a 10% discount on their mobile subscription if they signed up for the services are on average more favorable to the services than the other respondents.

We further note that the likelihood of using the ad services differs between countries, with Norwegians on average being least interested, followed by respondents in Serbia, Malaysia, and Pakistan. To test the significance of the differences between countries in Fig. 1, we use random effect ordered logit models with the countries serving as the explanatory variable. We separately estimate the model for respondents without a discount and then for respondents with a discount. Wald tests of the coefficients for all combinations of countries indicate that these differences are all statistically significant, with all p-values below 0.020.<sup>4</sup> Summing the main country difference from Fig. 1, we can see that Norwegians are less likely than respondents in the other countries to use the services offered both with and without discounts, while Pakistanis are more likely than the respondents in the other countries to use the services if given a discount.

Looking at the results from another perspective, respondents who are unlikely to use the service provide interesting information about the heterogeneity across the sample and between countries. For example, when Service 1 the least data-greedy service, is connected to a discount, this service is the most positively viewed in all four countries. However, 64% of Norwegians, 40% of Serbians, 31% of Malaysians, and 17% of Pakistanis declare that it is unlikely or very unlikely that they will use the service on our five-point scale. This suggests that there are significant differences in attitudes toward using such services within each country, and therefore that their consumer populations are highly heterogeneous. We also observe substantial differences between countries.

### 3.2. Ordered logit estimation to test behavioral predictions

Table 4 presents the random effect ordered logit estimations for the four countries separately. As discussed, the choice of model is based on the ordinal nature of the survey question and that the respondents each answered three likelihood questions, one for each service. It is important to note that it is not possible validly to compare the estimates of the ordered logit parameters between estimations. We use Stata 16 for all estimations. Service 2 serves as the base scenario in all estimations because this allows us to test Hypotheses 1 and 2 directly. A final qualification is that the measurement of our dependent variable (how likely it is that the respondent would use the service) is on an ordinal scale. Therefore, we are unable to consider the magnitudes of the coefficient estimates, only their direction and significance.

In what follows, we consider the results presented in Table 4 with respect to the behavioral predictions made in Section 2.3, looking especially at the differences between the likelihood of using the different services and the effect of the discount.

#### 3.2.1. The amount of personal data shared

We compare Services 1 and 2 to evaluate the scale effect, how the likelihood of using a personalized ad service changes when the service demands more personal data. From Table 4, we can see that the primary trend is that the willingness to use the ad service decreases with the level of data the users must share. In three of the four countries, Norway, Malaysia, and Pakistan, the respondents are significantly less likely to use Service 2 than Service 1 ( $p < 0.05$ ). The difference is that Service 2 requires sharing both location and browsing history, whereas Service 1 only requests location. In Serbia, there is no significant difference in the likelihood of use between the services.

Overall, the results in Norway, Malaysia, and Pakistan are in line with Hypothesis 1. They show that the willingness to share personal data decreases when consumers need to share more personal data in most countries. Nonetheless, even with the critical differences between only location data and when combining location and browsing data, the shift in responses from Service 1 to Service 2 is small (as illustrated in Fig. 1).

#### 3.2.2. Resharing personal data with other commercial actors

To test the scope effect, how the likelihood of using the ad service is affected when the number of actors that can access the personal data increases, we compare Services 2 and 3. The respondents are significantly more likely to use Service 2, where location and browsing history are only shared with the mobile operator, than Service 3, where the data are shared with other commercial actors in the two European countries Norway and Serbia ( $p < 0.01$ ). In Malaysia and Pakistan, we do not observe a significant change.

The results in Norway and Serbia correspond to Hypothesis 2. They show that, at least in the European countries in our study, the willingness to share personal data decreases when the mobile operator shares the data with retailers. Once again, as illustrated in Fig. 1, even though the results are statistically significant, they are small in an economic sense when we move from sharing information with the mobile operator alone to including third parties.

<sup>4</sup>  $W_{NO-SE \text{ no disc}} = 99.52, p = 0.00; W_{NO-SE \text{ disc}} = 89.76, p = 0.00; W_{NO-MA \text{ no disc}} = 247.80, p = 0.00; W_{NO-MA \text{ disc}} = 182.09, p = 0.00; W_{NO-PA \text{ no disc}} = 142.73, p = 0.00; W_{NO-PA \text{ disc}} = 533.63, p = 0.00; W_{SE-MA \text{ no disc}} = 33.14, p = 0.00, W_{SE-MA \text{ disc}} = 17.52; W_{SE-PA \text{ no disc}} = 5.40, p = 0.02; W_{SE-PA \text{ disc}} = 222.36, p = 0.00; W_{MA-PA \text{ no disc}} = 10.19, p = 0.00; W_{MA-PA \text{ disc}} = 122.91, p = 0.00$

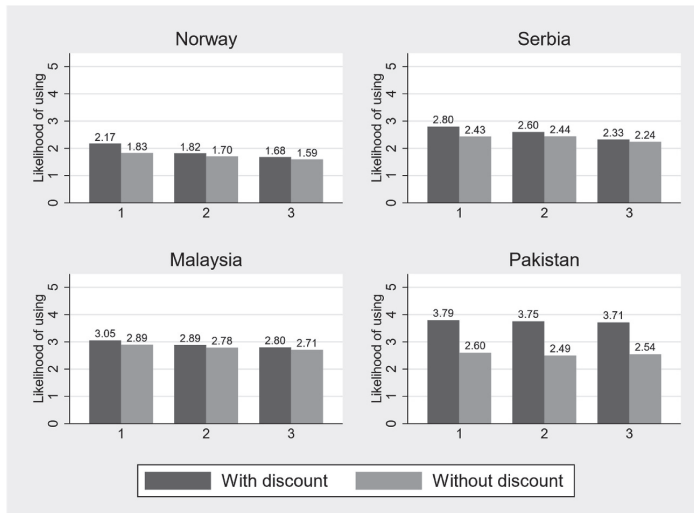


Fig. 1. Mean stated likelihood of use for each ad service. Note: Likelihood of use is measured on a five-point scale from 1 = very unlikely to 5 = very likely.

Table 4  
Likelihood of using the ad service—random effects ordered logit estimation.

Independent variables	Norway	Serbia	Malaysia	Pakistan
Service 1	0.58*** (3.45)	0.02 (0.11)	0.34* (2.50)	0.43* (2.46)
Service 3	-0.52** (-2.93)	-0.58*** (-3.71)	-0.24 (-1.78)	0.13 (0.77)
Discount and Service 1	1.25*** (4.73)	1.01*** (3.60)	0.42 (1.83)	4.72*** (12.38)
Discount and Service 2	0.68* (2.52)	0.42 (1.50)	0.33 (1.45)	4.95*** (12.89)
Discount and Service 3	0.60* (2.14)	0.22 (0.78)	0.25 (1.07)	4.65*** (12.21)
Age	-0.03 (-1.39)	-0.05* (-2.37)	0.07*** (3.54)	-0.04 (-1.41)
Female	0.06 (0.27)	-0.43 (-1.63)	-0.56** (-2.75)	2.82*** (8.39)
Level of concern	-1.02*** (-8.32)	-0.90*** (-6.48)	-0.72*** (-6.06)	-0.42* (-2.54)
Level of knowledge	-0.78*** (-5.64)	-0.41** (-2.78)	-0.92*** (-6.27)	-0.35 (-1.23)
Trust in mobile operator	0.39** (3.04)	0.46*** (3.41)	0.87*** (7.08)	0.57** (3.19)
N (three responses per respondent)	2401	2216	2426	2334

Notes: t-statistics in parentheses; \*p < 0.05, \*\*p < 0.01, \*\*\*p < 0.001.

3.2.3. Economic incentives

In general, the participants presented with offers including a 10% discount on their mobile subscription were more favorable toward the ad services than those without a discount. The effect of the discount is by far the most substantial in Pakistan (p < 0.001 for all three services). There is also a significant increase in the likelihood of use for all three services when offering a discount in Norway (p < 0.05). However, in Serbia the change with a discount is only significant for Service 1 (p < 0.001) and in Malaysia for non. All estimated parameters related to the discount, both significant and not, display their expected positive sign.

These results mostly support Hypothesis 3 and show that consumers in 3 of 4 countries are more willing to use an ad service that requires sharing personal data if given an economic benefit in the form of a discount on their mobile subscription. Hence, respondents are on average willing to make a tradeoff between personal data and money. However, as illustrated in Fig. 1, the differences are small in most countries except Pakistan.

For Norway and Serbia, we see that the effect of the 10% discount decreases as the services become more personal-data intensive. Typically, the discount effect is stronger for Service 1 than Service 2. This result is consistent with consumers evaluating the tradeoff between benefits and cost. The higher the cost in the form of sharing personal data, the smaller the number of respondents that find that a 10% discount is sufficient. Hence, for more personal-data-intensive services, the discount must be higher for as many to sign up for the service as the less data-demanding services. Again, Pakistan differs from the other countries where the 10% discount has approximately the same effect on all services.

### 3.2.4. Cross-country differences relating to concern, knowledge, and trust

We observe the most prominent differences between countries for *privacy knowledge*, with Norway 1.48 standard deviations above Pakistan, with Serbia and Malaysia in between (Table 2). Increasing levels of knowledge then result in significantly lower likelihoods of using a service in all countries except Pakistan, where the level of knowledge is deficient (Table 4).

There are also considerable differences in *trust in mobile operators* across countries (Table 2). Pakistan, which scores lowest on privacy knowledge, scores highest on trust in mobile operators. Malaysia scores lowest on trust, almost one standard deviation below Pakistan. For all four countries, we observe a positive relationship between trust in mobile operators and the likelihood that the respondents will use the services (Table 4).

For *privacy concern*, the two European countries score highest and the two Asian countries lowest, but the differences are minor compared with those for knowledge and trust (Table 2). For all four countries, we observe a negative relationship between privacy concern and the likelihood that respondents will use the services (Table 4).

## 4. Discussion and conclusion

This paper considered factors that affect consumers' willingness to share personal data with a commercial actor to obtain a personalized offer in Norway, Serbia, Malaysia, and Pakistan. Technological developments over the last decade have given consumers access to the Internet everywhere, facilitating access to fast data networks, smartphones, and social media. As a result, many commercial transactions in developed and developing countries now include transferring personal data from consumers to firms.

We find evidence that mobile Internet users aged 16–35 years care about their privacy when they encounter commercial actors. Many make tradeoffs in terms of how much data they are willing to share and with whom. Our survey results indicate that the willingness to share data decreases with the amount of data and the number of commercial actors that receive the data. The willingness to share also decreases with consumers' privacy concerns and privacy knowledge and increases with their trust in mobile operators. Furthermore, we find that small economic incentives increase the number of consumers willing to give up their data, especially in less wealthy countries. The results are in line with the findings in the privacy literature (Acquisti et al., 2020) and extend it by analyzing privacy in a mobile setting with location data and across a diverse set of countries.

By going beyond the typical WEIRD samples used in most digital privacy studies (Acquisti et al., 2020), this article provides new insights from non-WEIRD countries and the possibility of comparing WEIRD and non-WEIRD countries. While there are many similar preference patterns in the four countries studied, significant differences also require further attention. Our findings indicate that privacy insight generated in a WEIRD context is not necessarily valid outside that context.

The country differences are in line with expectations based on the economic and technological development of the four countries, as seen in the United Nations' Human Development Index and the Telecommunication Infrastructure Index. Norway is one of the world's wealthiest and most technologically developed countries, and few respondents were interested in the personalized ad service. Even with a 10% discount on their mobile subscriptions, less than 20% of young Norwegians were interested in the service.

In contrast, for Serbia and Malaysia, both middle-income countries, the share interested in the service was higher than in Norway, both with and without a discount. In these two middle-income countries in Europe and Asia, adding the discount on the mobile subscription resulted in about a third of young respondents being interested in the service. The poorest and least technologically developed of the four countries, Pakistan has the highest share interested in the service both with and without the discount. Three out of every four young Pakistani respondents were interested in the least data-greedy service with the discount. This suggests that consumers in developing countries are more likely to give up personal data to receive personalized offers. Adding a discount to the subscription strengthens this tendency.

Businesses that want to provide personalized services need to build trust with their customers, find a balance between well-targeted services and customers' personal space, and consider the economic benefits for the customers. Table 4 shows that those consumers who trust their mobile operators are more willing to use the ads service and share their data with the mobile operator. Less data-hungry services are met with a higher willingness to use than those demanding more personal data. Providing consumers with economic incentives increases the number of consumers willing to use the personalized services. Businesses using personal data as part of their business model need to know their customers' preferences in their context to ensure that they strike the best balance.

Our study fills a gap in the literature on privacy in non-WEIRD countries. However, the data is from 2017 and the personal data ecosystem is continuously developing, with new technology, market offerings, and regulations. One example of change is the strengthening of regulations of personal data in several developed countries in the last few years. The introduction of the EU's General Data Protection Regulation (GDPR) in 2018 affected our WEIRD country Norway. It is worth noting that people's attitudes may change slower than regulations and that the rapid development in digitalization and e-commerce have not reached all countries. A study by Wasenden (2020) of privacy concern and knowledge in Norway using data collected before and after the introduction of GDPR and the so-called Cambridge Analytica scandal (Isaak & Hanna, 2018), find only a minor change in privacy concern, while the change in privacy knowledge is more significant. The results from Wasenden (2020) move Norway, the WEIRD country in our study, further up

the ladder on privacy knowledge. For Pakistan, the least economically and technologically developed country in our study, recent articles by [Jamil \(2021\)](#) and [Imtiaz et al. \(2020\)](#) describe a slow digitalization and development in e-commerce, respectively. We find differences between the four countries, following the patterns of socio-economic and technology development. An interesting question for further research is whether privacy attitudes follow socio-economic and technology development over time.

Because of the complexity of digital privacy, individuals struggle to handle privacy issues, and there is a need for policy intervention and regulations in the form introduced by the European Union and Japan. Our analysis points toward another policy area that need attention — education. In our study, the level of knowledge on digital privacy issues is deficient in a large share of the population, and knowledge is negatively correlated with the likelihood of using the personalized service. Given the complexity of online data protection and the pace of digitalization, public and private actors should consider educational measures on digital privacy in all age groups.

**Declaration of competing interest**

None.

**Data availability**

The authors do not have permission to share data.

**Appendix 1**

Our analysis includes three knowledge and attitude measures: privacy knowledge, privacy concern, and trust in mobile operators. The instruments for privacy concern and privacy knowledge are mainly based on [Kobsa et al. \(2016\)](#), [Trepte et al. \(2015\)](#), and [Park and Jang \(2014\)](#). See [Evjemo et al. \(2020\)](#) based on the same data for more discussion on privacy knowledge, privacy concern, and trust in mobile operators in our context. Compared with [Evjemo et al. \(2020\)](#), we have re-estimated and standardized the variables for easy interpretation and comparison in our analysis.

[Table 5](#) presents the five items used as instruments for privacy concern. The items use a five-level scale going from “strongly agree” to “strongly disagree.” A confirmatory factor analysis gives a Cronbach’s alpha of 0.84, indicating that the items have a high degree of correlation. The privacy concern instrument is constructed using the Stata procedure for constructing latent variables and after that standardized across the whole sample to have a mean of zero and standard deviation of one.

**Table 5**  
Items in privacy concern instrument.

Statements to measure privacy concern
I am concerned that online companies are collecting too much personal information about me
It bothers me when I cannot control how my personal information is used by online companies
It usually bothers me when mobile applications ask me for personal information
I believe that mobile applications ask for more data than is needed to fulfill the purpose of the app
It bothers me that personal information given to online companies for a specific purpose can be used for other purposes

[Table 6](#) present the nine items used in the privacy knowledge instrument. They are measured through a five-point scale from “definitely true” to “definitely wrong.” A confirmatory factor analysis of the items results in a Cronbach’s alpha of 0.75, indicating that the items have an acceptable degree of correlation. The privacy knowledge instrument is constructed by taking the sum of the nine items before standardized across the whole sample to a mean of zero and a standard deviation of one.

**Table 6**  
Items in privacy knowledge instrument.

Knowledge statements
Facebook, Google, and similar companies track your activity on the Internet
Many mobile apps record your location
Social network site operators such as Facebook also collect information about nonusers of the social network site
When a mobile app has a privacy policy it means that no personal data are shared with other apps or companies
Facebook, Google, and similar companies delete personal data after a predefined period
App providers only collect personal information that is needed to deliver the service
When you deactivate GPS on your phone, your location cannot be tracked
Your browsing history is normally stored on your mobile phone
It is not possible to hack into private information on a mobile phone

We measure trust in mobile operators through one item “My mobile operator is trustworthy” with a five-point scale from “strongly

agree” to “strongly disagree.” Like the other two variables, this is also standardized across the whole sample with a mean of zero and a standard deviation of one.

## References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4), 736–758.
- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442–492.
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53.
- Benndorf, V., & Normann, H. T. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics*, 120(4), 1260–1278.
- Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters*, 117(1), 25–27.
- Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research*, 5(1), 62–70.
- Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., & McAuley, D. (2015). Personal data: Thinking inside the box. *Aarhus Series on Human Centered Computing*, 1(1), 4.
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer’s dilemma. *Information Technology Management*, 6(2), 181–202.
- Chen, P. T., & Hsieh, H. P. (2012). Personalized mobile advertising: Its key attributes, trends, and social impact. *Technological Forecasting and Social Change*, 79(3), 543–557.
- De Keyser, 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.
- Evjemo, B., Grønnevet, G., Ling, R., Nag, W., Røhr, H. L., & Wasenden, O. C. (2020). Privacy on smartphones. In R. Ling, L. Fortunati, S. S. Lim, G. Goggin, & Y. Li (Eds.), *The Oxford handbook of mobile communication and society* (pp. 563–579). Oxford: Oxford University Press.
- Haghirian, P., Madlberger, M., & Inoue, A. (2008). January. Mobile advertising in different stages of development: A cross-country comparison of consumer attitudes. In *Proceedings of the 41st annual Hawaii international conference on system sciences (HICSS 2008)* (48–48). IEEE.
- Imtiaz, S., Ali, S. H., & Kim, D. J. (2020). E-commerce growth in Pakistan: Privacy, security, and trust as potential issues. *Culinary Science & Hospitality Research*, 26(2), 10–18.
- Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51(8), 56–59.
- Jamil, S. (2021). From digital divide to digital inclusion: Challenges for wide-ranging digitalization in Pakistan. *Telecommunications Policy*, 45(8), 102206.
- Kobssa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An elaboration likelihood model approach. *Journal of the Association for Information Science and Technology*, 67(11), 2587–2606.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.
- O’Malley, L., Patterson, M., & Evans, M. (1997). Intimacy or intrusion? The privacy dilemma for relationship marketing in consumer markets. *Journal of Marketing Management*, 13(6), 541–559.
- Peppers, D., Rogers, M., & Dorf, B. (1999). Is your company ready for one-to-one marketing. *Harvard Business Review*, 77(1), 151–160.
- Rosenthal, S., Wasenden, O. C., Gronnevet, G. A., & Ling, R. (2020). A tripartite model of trust in Facebook: Acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology*, 23(6), 840–864.
- Schudy, S., & Utikal, V. (2017). ‘You must not know about me’—on the willingness to share personal data. *Journal of Economic Behavior & Organization*, 141, 1–13.
- Schwartz, P. M. (2019). *Global data privacy: The EU way* (Vol. 94, pp. 771–816). New York University Law Review.
- Segijn, C. M., Voorveld, H. A., & Vakeel, K. A. (2021). The role of ad sequence and privacy concerns in personalized advertising: An eye-tracking study into synced advertising effects. *Journal of Advertising*, 1–13.
- Spiekermann, S., Grossklags, J., & Berendt, B. (2001). October. E-Privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on electronic commerce* (pp. 38–47).
- Strycharz, J., van Noord, G., Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 13(2), Article 1.
- Taylor, C. R., & Carlson, L. (2021). The future of advertising research: New directions and research needs. *Journal of Marketing Theory and Practice*, 29(1), 51–62.
- Taylor, D. G., Davis, D. F., & Jilapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, 9(3), 203–223.
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “online privacy literacy scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law. Law, governance and technology series* (Vol. 20, pp. 333–365). Dordrecht: Springer.
- Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), 546–562.
- United Nations. (2020). *E-Government Survey 2020 - Digital Government In The Decade Of Action For Sustainable Development*. Retrieved from [https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20\(Full%20Report\).pdf](https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf).
- United Nations Development Programme. (2018). *Human development indices and indicators*. Retrieved from <http://hdr.undp.org/en/content/human-development-indices-indicators-2018-statistical-update>.
- Varian, H. R. (2010). Computer mediated transactions. *The American Economic Review*, 100(2), 1–10.
- Varian, H. R. (2014). Beyond big data. *Business Economics*, 49(1), 27–31.
- Wang, Y., Min, Q., & Han, S. (2016). Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. *Computers in Human Behavior*, 56, 34–44.
- Wasenden, O. C. (2020). Digitalt personvern – kunnskap, bekymring og atferd. *Magma*, (2), 64–73.
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389–418.
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89.

## **Paper 3**





# Privacy during Pandemics: Attitudes to Public Use of Personal Data\*

Eleonora Freddi<sup>1</sup> and Ole Christian Wasenden<sup>2</sup>

<sup>1</sup>Telenor Research and FAIR, The Choice Lab, Norwegian School of Economics

<sup>2</sup> Telenor Research and NMBU, Norwegian University of Life Sciences, School of Economics and Business

## Abstract

In this paper we investigate people's attitudes to privacy and the sharing of personal data when used to help society combat a serious contagious disease, such as COVID-19. Such attitudes are widely studied in commercial settings where the motivation is private gain, while studies at the societal level are lacking. Through a two-wave survey (April and November 2020) conducted in Norway and Sweden, we investigate the role of personal characteristics, and the effect of information, in shaping attitudes to privacy. We find that privacy concern is negatively correlated with allowing public use of personal data. Trust in the entity collecting data and collectivist preferences are positively correlated with this type of data usage. We find that providing more information about the public benefit of sharing personal data makes respondents more positive to the use of their data, while providing additional information about the costs associated with data sharing does not change attitudes. The analysis suggests that stating a clear purpose for the data collection and how the data will be used makes respondents more positive about sharing. By comparing the answers in two survey waves and two countries, we find that our results are robust across contexts and policy choices.

**Keywords:** Personal data; Privacy attitudes, COVID-19, Digital contact tracing

---

\*Emails: [eleonora.freddi@telenor.com](mailto:eleonora.freddi@telenor.com), [ole-christian.wasenden@telenor.com](mailto:ole-christian.wasenden@telenor.com).

# 1 Introduction

Due to the COVID-19 pandemic, the early 2020s will be remembered as a period of face masks, social distancing, lockdowns, and infection control measures. To help society implement efficient policies to control a disease, giving the health authorities access to highly personal information, such as people’s location and their physical contacts, could play an important role. For this reason, a large number of countries launched digital tracing apps and other measures that used personal data during the COVID-19 pandemic. People faced a situation in which they were promised a faster return to a normal life if they gave up part of their privacy and shared detailed personal data with the health authorities. Most people were used to disclosing personal data in a commercial setting when using an online service, but sharing data in order to help society was new to many people. Knowledge about people’s attitudes to such public use of personal data is still limited. Our paper presents evidence from a two-wave survey in Norway and Sweden that was intended to deepen our understanding of people’s attitudes to public use of personal data, when the purpose of sharing the data is to help society combat a serious contagious disease.

Being online is an integral part of modern life. In 2021, there were 4.2 billion active social media users and 5.2 billion unique cell phone users globally (Kemp, 2021). The providers of these digital services normally collect personal data from their users. The reasons for this practice range from enhancing users’ experience of the actual service to personalized marketing or selling the information to third parties. As regards the online users, however, it is not given that they are fully aware of how much personal data is gathered and how the data are used. Handling privacy, how personal data are harvested, stored, used, and shared while regularly using a large variety of online services, is a complex and difficult task (Acquisti et al., 2007, 2016, 2020; Athey et al., 2017; Gómez-Barroso, 2018; Solove, 2012). As suggested by the *privacy calculus theory*, users must be able to weigh the benefits of using a digital service against the risk that arises when surrendering personal data and reducing the private space (Dinev and Hart, 2006; Fox et al., 2021; Keith et al., 2013). Due to the intricacy faced by users of commercial digital services when encountering this trade-off, it is prohibitively difficult to reach desirable levels of privacy through individual actions alone (Acquisti et al., 2020).

Commercial actors are not the only entities that collect and use personal data. The public sector also launches online services that rely on data from citizens. One example of this is the health authorities’ use of digital tools to combat a pandemic, such as the one caused by COVID-19 (Budd et al., 2020). Such measures include the use of digital contact tracing apps, the gathering of cell phones’ locations to understand mobility patterns, and targeted

communication based on where people are. Such solutions were adopted by several countries in recent years in an attempt to reduce the spread of the COVID-19 disease. At the same time, discussions about privacy and the use of personal data linked to these digital tools was the subject of much public debate (e.g., Sweeney (2020); Kaya (2020)). When personal data are used for a public cause, such as disease control, the benefit of sharing data is not directly harvested by the individual who shares data. In such case, the privacy calculus would become even more challenging for the individual concerned, especially in a state of emergency. As a result, the gap between the desirable and achieved privacy levels may increase if the health authorities focus on the short-term health gains and underestimate the potential privacy cost (Rowe, 2020). Privacy concerns have indeed been one of the main obstacles to the adoption of public digital tools such as tracing apps (Chan and Saqib, 2021; Julienne et al., 2020; Pape et al., 2021). At the same time, the success of a tracing app relies on people being willing to share their personal data. Some tracing apps have failed precisely because of privacy issues, one example of which was the first version of the Norwegian app “Smittestopp”<sup>1</sup> Therefore, understanding people’s attitudes to public use of personal data is paramount if we are to shed light on their choice to share data with the authorities. This understanding is crucial to the success of such public digital tools.

The purpose of this paper is to bring new insights related to these privacy. We investigate whether people are positive about sharing data with health authorities when the benefits of data usage are harvested at the societal level. In particular, we study two research questions: (1) what role do personal characteristics play in shaping privacy attitudes? and (2) does providing information about the costs and benefits of data usage have an effect on privacy attitudes?

To answer these two research questions, we collected survey responses from Norway and Sweden in spring and fall 2020. First, respondents answered questions about their personal characteristics that could affect privacy attitudes: their concerns about privacy, their knowledge about privacy, their general trust in several companies and public agencies, as well as their preferences as regards government interventions and individual self-sacrifice. The latter measures are relevant given our context, where the benefit of sharing personal data is shared by everyone and goes beyond the self-interest of each individual. We then measured our outcome variable, namely whether respondents had positive or negative attitudes to different types of data collection by the health authorities. These questions were asked after randomizing the respondents into three groups as part of a survey experiment. We assigned respondents to different versions of an introductory text, which emphasized either the cost or

---

<sup>1</sup><https://techcrunch.com/2020/06/15/norway-pulls-its-coronavirus-contacts-tracing-app-after-privacy-watchdogs-warning/>

the benefit of personal data usage. A third group did not receive any additional information and was used as a control group.

We first analyze the relationships between privacy attitudes and personal characteristics. The variation across the different types of public data collection also makes it possible to analyze the effect of stating a clear purpose for the collection of personal data. Then, we analyze whether additional information about the costs related to an individual loss of privacy has a different effect on privacy attitudes than providing information about a common benefit in the form of public health gains. Both treatments are compared to the control group.

We find that being concerned about privacy and the handling of personal data is negatively correlated with attitudes to public entities using personal data. On the other hand, high trust in entities collecting information leads to more positive attitudes to the use of individual data. Strong collectivist preferences are also positively correlated with positive attitudes to public data usage. In addition, we do not find any significant relationship between privacy knowledge and privacy attitudes. Turning to the experiment, we find that respondents receiving information about the public health gains are more positive to public use of personal data than those in the control group. We find no significant effect of providing additional information about the individual costs of allowing personal data usage.

We interpret these results in light of the conjecture that, in a crisis situation like the one at the beginning of the COVID-19 pandemic, people would only respond to information suggesting that disclosing personal data would be part of the solution to the spread of the disease. As a result of the additional information about the public health benefits, the respondents realized that there was a clear purpose for sharing their personal data. This indicates that having a better understanding of the use of personal data by the entity collecting them would increase acceptance of the use of digital tools. Our descriptive analyses also indicate that stating a clear purpose for the use of personal data does affect people's attitudes to sharing them. Overall, these findings emphasize the importance of providing the right information when people have to decide whether to share personal data.

To check the robustness of our results against changes in contexts and policy choices that could have affected people's attitudes to privacy, we collected survey responses in two waves (spring and fall 2020) and from two neighboring countries (Norway and Sweden). Given the unexpected outbreak of COVID-19 in spring 2020, a feeling of emergency was widespread and people may have been more open to any solutions that could decrease its spread, even at the expense of their own privacy (European Data Protection Board, 2020). Six months later, when the situation around the pandemic outbreak was better understood, attitudes to privacy might have changed. In addition, the differences in policy choices between the two countries were large. From the onset of the pandemic, Norway imposed restrictions on

movement in public areas and on social gatherings, and schools, gyms, and restaurants were closed (Christensen and Lægheid, 2020; Helsingen et al., 2020; Sareen et al., 2021). Sweden, on the other hand, took a different path, with no face mask requirement and no quarantine for family members of infected people. Schools and gyms also stayed open and there was little contact tracing and testing (Vogel, 2020; Paterlini, 2020; Kampmark, 2021). Despite these contextual and institutional differences between the two survey waves and the two countries, we find that the results are surprisingly stable across the different samples, suggesting that privacy attitudes did not react to changes in either the context or the policy choices related to the use of personal data.

Our study contributes to the growing literature on the drivers and barriers of privacy attitudes. Privacy concern and trust are commonly investigated personal characteristics that could have an impact on privacy attitudes, mainly in a commercial setting (Acquisti et al., 2016, 2020; Baruh et al., 2017; Evjemo et al., 2020). Several recent studies have analyzed the relationships between these personal characteristics and the role of privacy in the adoption of COVID-19 tracing apps (e.g., Altmann et al. (2020); Chan and Saqib (2021); Julianne et al. (2020); Li et al. (2021); Thomas et al. (2020); Utz et al. (2021); Fox et al. (2021)). Other studies focus on whether people react differently to protect their privacy based on their preferences with respect to collectivism and paternalism (Munzert et al., 2021; Campos-Mercade et al., 2021). Our findings on privacy concern, trust in the health authorities and pro-collectivism are in line with evidence from these other studies. Fewer studies have looked at knowledge about privacy, which is key to making good decisions when trading privacy for a benefit. High privacy literacy has been found to be negatively correlated with willingness to share personal data in a commercial setting (Rosenthal et al., 2020; Alfnes and Wasenden, 2022; Bartsch and Dienlin, 2016). We are not aware of other studies that have investigated knowledge of privacy in the context of public use of personal data and the adoption of tracing apps.

The survey experiment contributes to understanding the effect of providing information on privacy attitudes and willingness to share data. Other studies have adopted similar experimental approaches and made similar findings as regards the effects of information (Julianne et al., 2020; Munzert et al., 2021; Trang et al., 2020). Unlike these studies, our treatment variation focuses specifically on the trade-off, which was key in the public debates, between the disadvantage of sharing personal data at the expense of one's own privacy and the advantage of using personal data for a public common good. It is known that there are large asymmetries in information between consumers and commercial actors, and it is generally difficult for people to make optimal decisions with respect to privacy (Acquisti et al., 2016, 2020; Athey et al., 2017). With the introduction of tracing apps and the societal benefits

of using individuals' personal data, this divergence has not lessened (Rowe, 2020). Overall, our study aims to address and guide the public discussion on the potential conflict between technologies using an increasing amount of personal data and the protection of individuals' privacy.

Finally, other studies have conducted longitudinal surveys, e.g., Simko et al. (2020). However, to enrich the analysis, we add a comparison between two countries that have taken very different approaches to handling the spread of COVID-19. Unlike Dennis et al. (2020) who look at how attitudes to governmental use of tracking data in an emergency differ across cultures, we chose to study two countries that share a great deal in terms of their cultural, political, and social background. The fact that Sweden did things differently from most comparable countries has been a point of discussion in many fields (e.g., Vogel (2020); Kampmark (2021); Andersson and Aylott (2020)). Our study adds to our knowledge about the possible effects of different governmental approaches and investigates whether the Swedish strategy affected people's attitudes and behavior in the privacy sphere.

## 2 Background and hypotheses

The point of departure for our analyses is the choice that individuals face of whether to use a voluntary digital tool, such as a tracing app, that requires the collection and use of personal data by the health authorities. According to the *privacy calculus theory*, to make such a decision, people must weigh the benefits of using the tool against the cost of disclosing their personal data (Dinev and Hart, 2006; Fox et al., 2021; Keith et al., 2013). Most commonly in the privacy literature, benefits linked to sharing personal data are related to a single individual. The benefit is often a payment to the individual if they give away their data (Benndorf and Normann (2018); Grossklags and Acquisti (2007) or personalized ads and an additional discount on their cell phone bill (Alfnes and Wasenden, 2022)). However, in the case of a pandemic, detailed information about people's location, their health status and their contacts could help an entire population, and the benefits of sharing information therefore go beyond pure self-interest. Our study differs from the existing literature along two dimensions. First, we elicit attitudes in a context in which a public entity, rather than a commercial actor, is collecting and using personal data. Second, we investigate whether we find predictions for personal characteristics related to privacy attitudes and for the effects of information provision that are similar to those we would expect from a purely individualistic motivation for sharing data.

Previous literature focusing on private benefits of protecting privacy has identified non-negligible relationships between privacy concern and privacy knowledge, on the one hand,

and privacy attitudes, on the other (Rosenthal et al., 2020; Evjemo et al., 2020; Alfnes and Wasenden, 2022). Worries that personal data could be misused are likely to be negatively correlated with willingness to share the information in question. Knowing how companies or public entities collect and handle personal data increases awareness about what type of information people are willing to share. Trust has been found to be an important driver of willingness to share personal data (Altmann et al., 2020; Julienne et al., 2020; Simko et al., 2020). With respect to privacy, there is often an information asymmetry between companies or public entities and people, with the latter usually having incomplete information about the use of their personal data. Trust in the company or entity that is collecting the data can play an important role in the individual being willing to share data despite a lack of information. In the context that we analyze, the benefit of sharing personal data is spread between more individuals and goes beyond the pure self-interest of each individual. Consequently, it is natural to explore whether respondents react differently based on their preferences as regards collectivism and paternalism (Munzert et al., 2021; Campos-Mercade et al., 2021). People who are more positive about government interference, and who value group interests above their own, are more likely to be positive about letting a public entity use their own personal data when it is to be used for a public common good. To investigate our first research question on the relationships between personal characteristics and attitudes to sharing personal data, we propose the following hypotheses:

**Hypothesis 1** *Being concerned about privacy is negatively correlated with allowing the use of personal data by the health authorities.*

**Hypothesis 2** *Having knowledge about privacy is negatively correlated with allowing the use of personal data by the health authorities.*

**Hypothesis 3** *Trust in the health authorities is positively correlated with allowing their use of personal data.*

**Hypothesis 4** *Collectivist preferences are positively correlated with allowing the use of personal data by the health authorities.*

Another important aspect of understanding privacy attitudes is the effect of information on the cost-benefit trade-off. The provision of information about the benefits and costs of sharing personal data has been found to affect people's propensity to disclose personal data (Marreiros et al., 2017). However, the highlighted positive and negative features of privacy

both belong to the private sphere of individuals. Thus, it is not straightforward to conclude that we would find the same results when emphasizing a private cost versus a common benefit for society as a whole. To address our second research question, we formulate the following hypothesis on the effect of information:

### **Hypothesis 5**

- (a) *Respondents receiving information about the privacy cost are more negative about allowing the use of personal data by the health authorities compared to respondents in the control group.*
- (b) *Respondents receiving information about the public health gains are more positive about allowing the use of personal data by the health authorities compared to respondents in the control group.*

Given the emphasis on information, it is also interesting to gain a better understanding of how a clear description of the purpose of the data collection affects attitudes to sharing. We take a tracing app as an example, the purpose of the which is to contribute to efficiently combating the disease. At the individual level, this is achieved through warning systems via the app, where people will receive information if, for example, they have been in contact with someone who carried the virus. Being explicit about the grounds for these warnings could facilitate adoption and use of the app. In our survey, we vary the descriptions of different potential types of data collection by the health authorities, making it possible to analyze whether stating a clearer purpose for the data gathering is associated with more positive privacy attitudes.

Finally, sentiment about sharing personal data may change due to the specific context in which the data is collected, and it may be susceptible to other external factors that could justify the use of the data. A situation in which health authorities wanted to use personal data from the general public to combat a contagious disease was new to most people at the outbreak of the COVID-19 pandemic. This makes it worth investigating whether the evidence in support of our hypotheses is susceptible to changes in contexts and institutional differences. In particular, by running two waves of the survey, we focus on two different periods in the pandemic development, and by collecting responses in both Norway and Sweden, we examine differences in policy choices related to the pandemic.

In the early phases of the pandemic, when the first wave of the survey was conducted, there was a strong feeling of urgency, and it is likely that any solutions available to stop the



spread of the disease would have been welcomed by the public. Uncertainty surrounding the spread of the disease was very high, and many countries were exploring several solutions that involved the use of personal data in an attempt to reduce infection rates. Six months into the pandemic, when the second wave was conducted, the situation was somewhat more manageable and, even though infection rates were still high, the sense of urgency had decreased. Other non-pharmaceutical interventions were implemented across the world and the use of personal data in the fight against the pandemic became less crucial. Thus, the context in which the survey was presented to the respondents was quite different in the two waves, and this change may have affected privacy attitudes. We conjecture that, in the second survey wave, privacy concerns may have outweighed the potential benefits of sharing personal data.

Besides better management of the pandemic, we also examine any differences between countries that arose because they pursued different strategies. From the very beginning of the pandemic, Norway imposed restrictions on movement in public areas and social gatherings, and schools, gyms, and restaurants were closed (Christensen and Læg Reid, 2020; Helsingen et al., 2020; Sareen et al., 2021). Discussions of the public use of personal data were very common in the media and in political debates (Sandvik, 2020). These debates were fomented by a feeling that it was a matter of urgency to find a solution to stop the spread of the disease. Sweden took a different path than most comparable countries: no face mask requirements and no quarantine of family members of infected people were imposed, schools and gyms remained open, and there was little contact tracing (people who became infected should call their own contacts instead) and little testing (Vogel, 2020; Paterlini, 2020; Kampmark, 2021). Most of the responsibility for social distancing, following hygiene measures, and reducing the number of one's contacts was left to the voluntary choice of the Swedish people themselves (Vogel, 2020; Paterlini, 2020). This very different strategy was already part of the public debate when the first wave of the survey was conducted, and many people regarded the Swedish approach as controversial (Paterlini, 2020). This lenient approach resulted in a heated debate among scientists in Sweden, which nonetheless did not decrease trust in the authorities among the Swedish population (Helsingen et al., 2020). The use of personal data was not considered to be part of the strategy for combating the disease and, most importantly, the spread of the disease was not perceived as an immediate threat to society (Kampmark, 2021; Vogel, 2020). Against this background, our conjecture is that respondents in Sweden would be more reluctant to allow the use of personal data by the health authorities than respondents in Norway.

### 3 Sample and survey design

#### 3.1 Sample

The first survey wave was conducted in collaboration with the global market research agency Kantar in April 2020 in both Norway and Sweden. We collected responses from 2587 respondents: 1387 from Norway and 1200 from Sweden. The samples in both countries are relatively representative of the working population, with a bias towards respondents with higher education (see Table 1). Respondents who agreed to be re-contacted at a later stage responded to the same questions in a second survey wave, which was conducted in October–November 2020. In Norway, 958 respondents completed both waves and 945 did so in Sweden. Attrition was not random, but it did not affect responses to the survey questions and there are no significant differences between respondents completing only the first wave and those completing both waves for all other questions in the survey. More details on attrition are provided in the Appendix section B and in Table A.1.

Table 1: Background characteristics of the survey sample

	Mean	Std. Dev.	Median	N	Pop NO	Pop SE
Age	48	16.79	48	2587		
Female	0.50	0.50	1	2587	0.50	0.49
Higher education	0.61	0.49	1	2587	0.35	0.38
Employed	0.64	0.48	1	2581	0.58	0.68
Living alone	0.22	0.41	0	2587	0.18	0.19
Household income	1.95	0.79	2	2226		

*Notes:* The table lists background characteristics of the pooled sample with respondents from both Norway and Sweden. “Higher education” is an indicator taking value 1 if the respondent has a post-secondary education. “Employed” is an indicator taking value 1 if the respondent is in full or part-time employment. “Living alone” is an indicator taking value 1 if the respondent is living alone. “Household income” is a categorical variable taking value 1 if the respondent has a low income, 2 for a middle income and 3 for a high income. The last columns report averages from Statistics Norway and Statistics Sweden, respectively. The shares from the official statistics have been calculated based on the same age range as the sample (17-74 in Sweden and 18-88 in Norway), except for “Living alone”, which is calculated for the entire population.

## 3.2 Survey questions

**Survey structure.** The surveys were conducted in Norwegian in Norway and in Swedish in Sweden. Respondents were informed that the purpose of the survey was to determine their attitudes to privacy and their willingness to share personal data with the health authorities, with the aim of combating a contagious disease. The survey took approximately 15 minutes and consisted of three parts. In the first part, respondents answered questions about some personal characteristics that could affect privacy attitudes. These questions were asked at a general level and were not specifically linked to health authorities and disease control. The second part of the survey focused on attitudes to public use of personal data. These questions formed the basis for our outcome variable on privacy attitudes. Respondents were first presented with a short text describing a situation in which the health authorities needed to use individuals' personal data, such as location, to combat an infectious disease. In this part of the survey, we implemented the survey experiment, where respondents were randomly assigned to receive additional information about either the privacy cost or the public health gains of sharing personal data. A control group did not receive any additional information. After reading the introductory text, the respondents were asked about their attitudes to the health authorities collecting and using personal data. In the third part, we asked about attitudes to the use of a mandatory versus voluntary cell phone tracing app, and their attitudes to their cell phone operator using and sharing personal data with the health authorities.<sup>2</sup> We obtained information about the respondents age, gender, education, living conditions, employment status, and income through the market research agency.

**Personal characteristics.** We gathered data that enabled us to measure privacy concern, privacy knowledge, trust in different actors, as well as preferences as regards paternalism and individual self-sacrifice. For privacy concern, we first created an index combining the responses to three statements about worries about a potential misuse of personal data. Based on the index, we constructed an indicator variable that takes value 1 if the respondents have a value for the concern index higher than the average for the sample they belonged to. To measure privacy knowledge, we use five statements about the handling of personal data that are either true or false. We construct an indicator variable that takes a value of 1 if the respondents, on average, have correctly or almost correctly answered all five questions.<sup>3</sup> From

---

<sup>2</sup>Since the focus of this study is on investigating attitudes to the use of personal data by public entities, we exclude these questions from the analyses.

<sup>3</sup>For the five statements on privacy knowledge, we use a five point scale: "definitely true", "probably true", "I don't know", "probably false", "definitely false". The answers to each statement are recoded to range from 2 to -2. A value of 2 means that the respondents have correctly guessed the answer to a statement. A value of 1 means that the respondent answered, for example, "probably true" to a true statement. If the

the question on trust in the health authorities, we constructed an indicator variable that takes value 1 if the respondents agree or strongly agree that the agency is trustworthy. Finally, we combine the responses to four questions about government interventions and individual self-sacrifice in an index, and define respondents as “collectivist” if they have a value for the index that is above the average for the sample they belong to. More details on these survey questions and the construction of the indexes and variables are provided in the Appendix section C, as well as in Tables A.2 and A.3.

**Survey experiment on the effect of information.** The respondents were randomly assigned to a *Privacy cost* treatment group, a *Public health gain* treatment group, or a control group. The three groups received different versions of the text about the health authorities’ use of personal data. It was explained to all three groups how location data are processed and collected, either through cell phone base stations or through GPS functionalities present on their cell phones. Respondents in the *Privacy cost* treatment group were presented with a sentence highlighting that sharing personal data comes at the expense of individuals’ own privacy and that the right to privacy is part of human rights. A different sentence was presented to respondents in the *Public health gain* treatment group. This second treatment focused on the necessity to collect location data to efficiently combat the disease and consequently to save lives. The experimental design created exogenous variation between respondents as regards the information on the use of personal data, before they answered about their attitudes to such use.

The randomization was effective overall. Respondents are balanced between the three groups with respect to demographic background information in Norway. In Sweden, we find that, among respondents in the *Public health gain* group, there is a higher share of highly educated individuals compared to the other two groups, and that the *Privacy cost* group has a lower share of respondents living alone compared to the other two groups. When considering the categorical variables for education and living conditions, we find no significant differences across the three groups. Further details are provided in Table A.4. To take into account any potential bias, we add these demographics characteristics as controls in our analyses.

**Attitudes to public use of personal data.** After receiving information about the collection and use of personal data, respondents were asked whether they were positive about the health authorities collecting and using the data to combat a contagious disease. To gain insight at a detailed level, we asked about seven different types of data collection. In particular, respondents have a total score of 5 points, they are classified as being privacy knowledgeable.

we focused on different levels of privacy intrusion, starting with more anonymous personal data and moving towards more individual and personalized information (e.g., tracking of movements and health status). For three types of data gathering, we introduced a specific purpose for the use of the personal data. For example, the gathered data would make it possible to send warnings when an individual has been in contact with infected persons or when they are breaking quarantine rules. More details about the different types of data collection are provided in the Appendix section D. To ensure that we have a single measure for these attitudes to the use of personal data, we construct an index (*Privacy attitude index*) by summing the standardized version of the seven variables.<sup>4</sup> The Cronbach's alpha for the index is between 0.93 and 0.94 across the four samples (two waves in Norway and two in Sweden), indicating strong internal consistency. Summary statistics for the index are reported in Table A.5 and A.6.

## 4 Results

In this section, we will present the results of our empirical analyses. We use the pooled sample with data from both Norway and Sweden from the first survey wave (spring 2020) to test Hypotheses 1-4 on the personal characteristics shaping privacy attitudes, and to test Hypothesis 5 on the effect of information provision. In section 4.4, we discuss the evidence for whether the findings hold separately in Norway and in Sweden, and in the second survey wave.

### 4.1 General trends in privacy attitudes to public use of personal data

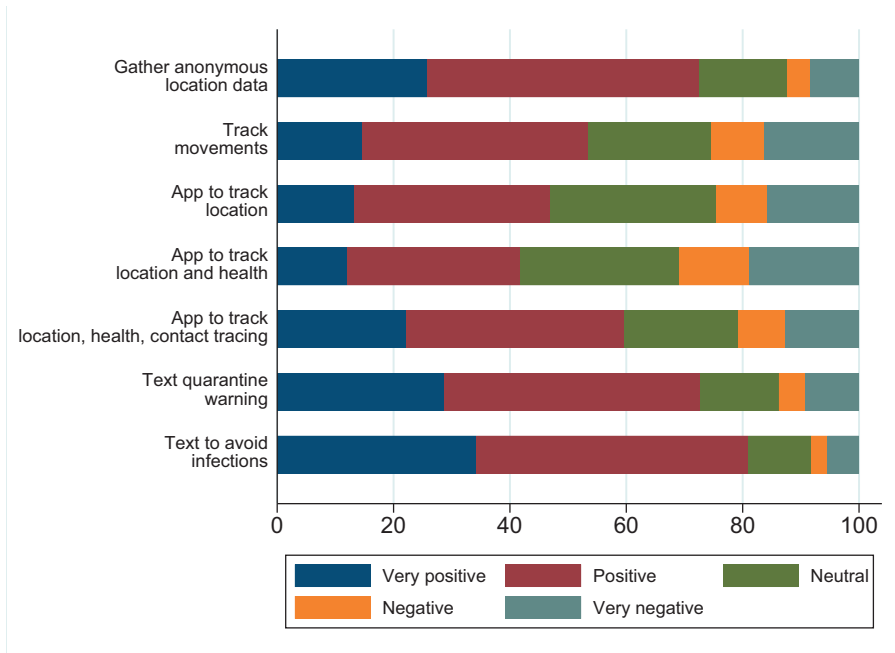
First, we look at the general patterns in the attitudes to the use of personal data by the health authorities in our context of combating a contagious disease. Figure 1 shows the distribution of responses relating to these privacy attitudes for the seven different types of public data gathering (more details are provided in Table A.5). We observe that the share of respondents that are either positive or very positive varies substantially across the different types of data collection. It ranges from around 42 percent for an app that tracks location and health status to 81 percent for sending text messages asking people to leave an area to avoid infection. Overall, respondents have less positive attitudes to more privacy-intrusive data collection. For example, they are more positive about the *gathering of anonymous location*

---

<sup>4</sup>We construct the standardized variables using the mean and standard deviation of the respondents in the control group in our survey experiment.

data compared to *tracking of personal movements*. Similarly, the attitudes were less positive about an app that *tracks location and health status* compared to one that only *tracks location*. This indicates that, also in cases when personal data are used for a common benefit, a larger share of people have negative sentiments as the data become more privacy intrusive.

Figure 1: Distribution of responses concerning attitudes to public use of personal data



*Notes:* The figure shows attitudes to seven types of data collection by the health authorities. The first two types involve gathering location data through cell phone networks. Then, there are three types launching an app to trace personal data that entail different levels of privacy intrusion. Finally, there are two types of data collection involving the use of text messages to warn against rule infringements during quarantine and to leave areas to avoid infection. The graph is based on the pooled sample with data from both Norway and Sweden in spring 2020, N=2556.

In Figure 1, we also observe an interesting pattern indicating that stating a clear purpose for the use of the personal data makes respondents more positive. Focusing on the three different types of data collection including a tracing app, the share of respondents that are either positive or very positive about this app starts at a fairly low level of 47 percent for

the app that tracks location. The share of positives falls to 42 percent when use of the app becomes more intrusive by including tracking of health status. However, when we introduce a private benefit for the most intrusive version, i.e., receiving a warning if one has been in contact with an infected person, the share of positives increases to 59 percent. Similarly, when presenting the types of data gathering where the health authorities send out location-based text messages, a clear private benefit is again specified, and we find very high shares of positive or very positive attitudes, at 73 and 81 percent, respectively. Despite these differences across the different types of data collection, we combine them in the *Privacy attitude index* (as described in section 3.2), which will serve as our outcome variable in the main analyses.

## 4.2 The role of personal characteristics

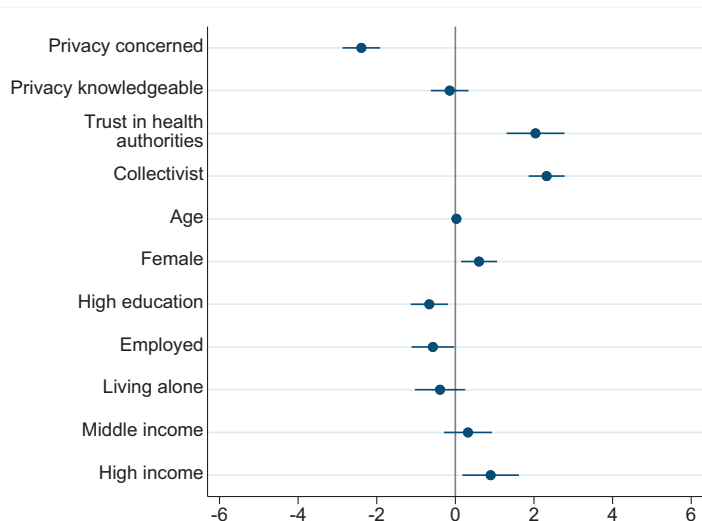
To answer our first research question, we test the predictions concerning personal characteristics shaping privacy attitudes, as defined in Hypotheses 1-4. In particular, we investigate whether the relationships found in the literature on commercial transactions also hold in a setting where personal data can be used for a public good. More specifically, we focus on whether privacy concern and privacy knowledge, trust in the health authorities, and collectivist preferences are correlated with privacy attitudes in our public setting. Using the pooled sample from the first wave (spring 2020), we regress the indicator variables for the four personal characteristics on the *Privacy attitude index*.<sup>5</sup> We also include demographic control variables for age, gender, level of education, employment status, living conditions, and household income. The results are reported in Figure 2 (more details are provided in Table A.7).

Overall, we find support for Hypothesis 1, 3, and 4, but not for Hypothesis 2. In line with Hypothesis 1, we find a negative relationship between privacy concern and the *Privacy attitude index*, suggesting that respondents who worry about their privacy are also more reluctant to allow the use of their personal data in a context of public importance. Being concerned about privacy reduces the privacy index by 2.39 units (a difference of 0.42 of a standard deviation) compared to being non-concerned.<sup>6</sup> On the other hand, the role of privacy knowledge is less straightforward. Even though we find a negative correlation with the *Privacy attitude index*, the coefficient is not significant. The role of privacy knowledge seems to be limited and we do not find evidence in support of Hypothesis 2. Turning to trust, we find a positive relationship with the *Privacy attitude index*, in line with Hypothesis 3: the more trust in the health authorities, the more people are willing to let a government agency

<sup>5</sup>The results for each country and for the second wave are analyzed in section 4.4.

<sup>6</sup>The standard deviation of the index is 5.75, and it ranges from a minimum of -16.19 to a maximum of 10.13. Summary statistics for the attitude questions and the index are provided in Table A.5

Figure 2: Relationships between personal characteristics and the *Privacy attitude index*



*Notes:* The figure reports coefficient estimates with 95% confidence intervals from a linear regression of personal characteristics (privacy concerned, privacy knowledgeable, trust in the health authorities, collectivist preferences) on the Privacy attitude index. Demographic controls are included. Positive (negative) coefficients are associated with an increase (decrease) in the privacy attitude index. The analysis is carried out on the pooled sample with responses from both Norway and Sweden in the spring of 2020 for respondents with full demographic information, N=2206.

use their personal data. Having trust increases the privacy index by 2.0 units. Finally, we find a strong and positive relationship between the *Privacy attitude index* and collectivist preferences, increasing the index by 2.3 units. In support of Hypothesis 4, people who are more positive about government interventions, and who are willing to put group interest before their own, are more willing to allow use of their personal data when the data are used for a public good.

### 4.3 The effect of information

To answer our second research question and test Hypothesis 5 on the effect of information, we use the survey experiment to analyze whether providing information about the public health gain and privacy costs can have an effect on attitudes when the context for sharing the data



involves a common good. First, we regress the indicator variables for the two information treatments compared to the control group on the *Privacy attitude index*.<sup>7</sup> The findings from the survey experiment are reported in Table 2.

In contrast to the predictions in Hypothesis 5a, we do not find a negative effect of the *Privacy cost* information on attitudes to the use of personal data compared to the respondents in the control group. However, for the second information treatment on *Public health gain*, we find a significant positive effect in line with Hypothesis 5b. More information on the pro-social purpose can lead to more positive attitudes to data sharing. In particular, receiving additional information that the sharing of personal data could help save lives increases the *Privacy attitude index* by 0.8 units (a change of 0.14 of a standard deviation) compared to respondents in the control group.

Given the correlations between privacy attitudes and the personal characteristics discussed in section 4.2, we include the indicator variables for being privacy concerned, privacy knowledgeable, having trust in health authorities, and being collectivist as controls in the analysis of the effect of information on privacy attitudes. The findings, reported in column (2) of Table 2, confirm a positive effect of providing information about the public health gains. This effect is only significant at a 5 percent level and the magnitude of the effect is reduced (an increase of 0.6 units for the privacy index).<sup>8</sup> Finally, the results are robust when adding a set of demographic controls, as shown in column (3) of Table 2. We conclude that we do find a positive impact of providing information about a public health gain of using personal data, while we do not find a significant effect of providing information about the privacy cost.<sup>9</sup> Like the descriptive results on more positive attitudes when indicating a clear purpose discussed in section 4.1, the experimental results suggest that the provision of information plays an important role in the formation of privacy attitudes, when a precise aim for the use of the data is stated.

---

<sup>7</sup>We run the analysis for the pooled sample of the first survey wave. The results for each country and for the second wave are analyzed in section 4.4.

<sup>8</sup>The regression results with interaction terms between the information treatments and the four personal characteristics are insignificant, with one exception. Respondents in the group that receives more information about the privacy cost are more positive about public use of personal data than the control group. The results for health gains were weaker when we introduced the interactions, but still significant at a 10 percent level.

<sup>9</sup>We have tested whether there is a difference between the two treatments by running the same regression without the control group, and found no such difference. Details of the regression are given in A.8.

Table 2: The effects of information provision on privacy attitudes

Dep. var.:			
Privacy attitude index	(1)	(2)	(3)
<i>Treatments</i>			
Privacy cost	0.536 (0.276)	0.454 (0.261)	0.438 (0.281)
Public health gain	0.816** (0.280)	0.623* (0.265)	0.724* (0.285)
<i>Personal characteristics</i>			
Privacy concerned		-2.302*** (0.226)	-2.358*** (0.243)
Privacy knowledgeable		-0.496* (0.217)	-0.137 (0.243)
Trust in health authorities		2.276*** (0.356)	2.027*** (0.375)
Collectivist		2.269*** (0.216)	2.318*** (0.234)
<i>Demographic controls</i>			
Age			0.028*** (0.007)
Female			0.612** (0.233)
Higher education			-0.680** (0.241)
Employed			-0.560* (0.278)
Living alone			-0.398 (0.326)
Middle income			0.295 (0.312)
High income			0.869* (0.368)
Constant	-0.000 (0.200)	-1.782*** (0.394)	-2.849*** (0.684)
Mean Privacy attitude index	0.453	0.453	0.453
Observations	2587	2571	2206
Adjusted $R^2$	0.003	0.111	0.122

*Notes:* The table reports OLS coefficients of regressing the information treatments on the *Privacy attitude index* for the full sample, combining Norway and Sweden in the first wave. The treatments “Privacy cost” and “Public health gains” are compared to the control group. In column (2) we add personal characteristics and in column (3) we also include a set of controls. Standard errors are in parenthesis. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

#### 4.4 Robustness of the results to contextual and institutional differences

Our data make it possible to compare the respondents' attitudes at different points in time, when the context for the use of personal data changed, and between two similar countries, Norway and Sweden, which chose quite different measures to control COVID-19. Figure 3 shows the share of respondents that are positive or very positive to each of the seven types of data collection, split between both countries and survey waves. The main picture is that the shares are quite similar across both time and country.

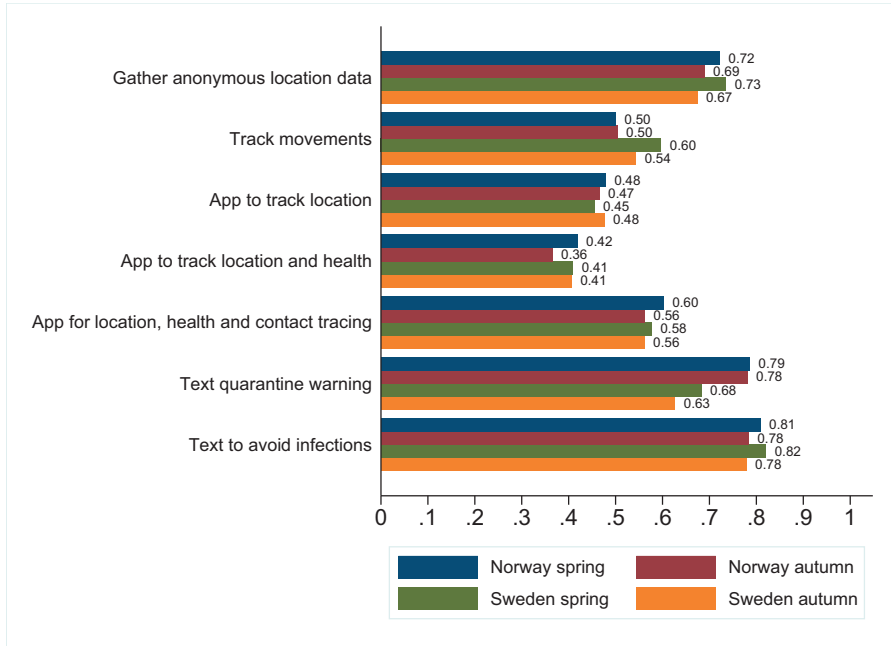
As described in section 2, the two survey waves were conducted during two periods that most likely differed in terms of the prevailing perception of the COVID-19 disease and in the strategies available to stop its spread. The feeling of uncertainty and urgency had most likely decreased six months into the pandemic, and it was known that vaccines would shortly become available, thereby offering an alternative solution to tracing personal data. Thus, it is possible that the general sentiment about the public use of personal data was different a few months into the pandemic compared to the very early stages. We start by comparing attitudes during the two waves of the surveys. Figure 3 shows the similarity in the shares of respondents who are positive or very positive in the two waves in each country (more details are given in Table A.6). Nor do we find differences in the correlations between personal characteristics and the *Privacy attitude index* (more details in Table A.9). The only exception is the role of trust in the health authorities, which, in Sweden in the first survey wave, has a smaller and less significant relationship with privacy attitudes. Finally, with respect to the effect of information, we do not find different effects of the treatments between the two survey waves (more details in Table A.10).<sup>10</sup>

Turning to potential country differences, as discussed in section 2, Norway and Sweden chose different strategies to limit the spread of COVID-19, and the interventions (or lack of them) implemented in each country influenced people's awareness and overall impression of the pandemic (Andersson and Aylott, 2020; Helsingen et al., 2020; Sareen et al., 2021). Figure 3 again shows quite similar attitudes to each of the seven types of data collection in the two countries in both spring and fall 2020 (see Table A.6 for more details). Despite the differences in governmental approach, this does not seem to have influenced how people perceived the use of personal data by a public entity. Moreover, with the exception of trust in Sweden in the first wave, the relationships between the personal characteristics and privacy

---

<sup>10</sup>The OLS estimates from the two separate regressions per survey wave are similar and, when running a regression on the pooled data for both waves, the interaction terms between the treatment variables and survey waves are not significant.

Figure 3: Comparison of shares of positive attitudes to public use of personal data in the two survey waves



*Notes:* The figure shows the shares of positive attitudes to several types of data collection by the health authorities that involve gathering and using personal data, in each round in each country. The first two types of data collection refer to gathering location data through cell phone networks. Then, there are three types that refer to launching an app to trace personal data that involve different levels of privacy intrusion. Finally, there are two types of data collection involving the use of text messages to warn against rule infringements during quarantine and to leave areas to avoid infection. Panel (a) shows responses from the two survey waves in Norway. Panel (b) shows responses from the two waves in Sweden.

attitudes are stable across the two countries (more details in Table A.9). However, we do find some differences between Norway and Sweden with respect to the information treatments (details provided in Table A.11). While the results from Sweden from both survey waves mimic the findings from the pooled sample, in Norway we do not find significant results for the *Public health gain* treatment. The reason could be that general privacy concerns, high

trust in the health authorities, and positive attitudes to collectivist approaches have had a stronger influence than an emphasis on the health gain itself. These results for Norway are in line with evidence from Munzert et al. (2021) and Julienne et al. (2020), who find that providing additional information and appealing to the common good do not increase the consensus on using tracing apps in Germany and in Ireland, respectively.<sup>11</sup>

From these comparative analyses, we conclude that privacy attitudes are relatively robust to changes in both contexts and policy choices. Other factors and preferences that affect privacy attitudes do not tend to vary and their relationships with the sentiment about the public use of data are constant. Our information interventions do not seem to have played a major differential role across time, and we find some effects for Sweden, but not for Norway.

## 5 Discussion and concluding remarks

In our increasingly digital lives, understanding attitudes to privacy and the handling of personal data is crucial not only to develop appropriate technology, but also to implement regulations and suggest policies that are in line with people's preferences. The COVID-19 pandemic and the attempts to limit the spread of the disease by digital means added a new layer to the complexity of privacy. Striking a balance between the use of personal data and the protection of individuals' privacy became even more difficult for the individual. Detailed information about people's location and health status could play a crucial role in combating the pandemic. Consequently, the benefits of sharing personal data could go beyond individual self-interest. If an individual shared personal data with the health authorities, society could gain. Our study aims to deepen our understanding of privacy attitudes, their formation and what could drive changes in sentiment, when the benefit is harvested at the societal level.

For a digital tool like a tracing app to become successful, a large share of the population must be willing to use it. The insights from this study, which give us a better understanding of the formation of attitudes to tools like tracing apps, are important in the design of such tools. Taking peoples' attitudes into account when planning and implementing a digital tool that uses personal data for the common good is necessary in order to achieve high take-up rates and become a success. Firstly, we find support for three of our four hypotheses related to the role of personal characteristics. The hypotheses were based on findings from studies in commercial settings, and we tested them in a context where the data are used to serve a public cause. Several other studies have looked at privacy attitudes in the context of the

---

<sup>11</sup>Trang et al. (2020) similarly find a larger intention to install a tracing app when a societal benefit is highlighted compared to a benefit for the individual. However, their experimental design does not include a neutral category where the purpose of the application is not discussed.

COVID-19 pandemic and the use of tracing apps. Being concerned about privacy is negatively correlated with willingness to adopt a tracing app (e.g.,Julienne et al. (2020); Simko et al. (2020); Trang et al. (2020)), while high levels of trust in the government and other public entities lead to more positive attitudes (e.g., Altmann et al. (2020); Julienne et al. (2020); Simko et al. (2020)). Our findings are in line with these results. We also find evidence consistent with other studies on the positive role of preferences for government interventions and more collectivist approaches (Munzert et al. (2021); Campos-Mercade et al. (2021)). It is likely that the public sector can contribute to establishing low levels of privacy concern and high levels of trust through transparency and good handling of personal data over time. However, these mechanisms are not well understood, and more research is needed.

With respect to privacy knowledge, people with weak privacy competence could be more willing to share data in a commercial setting, as they are not capable of evaluating the privacy costs (Rosenthal et al. (2020); Trepte et al. (2015); Alfnes and Wasenden (2022)). To our knowledge, no previous study has looked at privacy literacy as a relevant factor in relation to sharing personal data for a public common good. However, we do not find that being privacy knowledgeable has any significant relationship with attitudes to personal data usage. We conclude that concern about, rather than knowledge of, how personal data might be used (and misused) is a much bigger barrier to having a positive attitude to sharing data for a public cause.

From our analyses, we can also conclude that information plays an important role. Giving those who are asked to share their personal data proper information and a clear description of the purpose of the data gathering and usage has an impact on privacy attitudes. The more clearly the purpose is described, the more positive are attitudes. It follows that, when planning to launch a service like a tracing app, the importance of clear communication with the general public should not be underestimated. Communication and providing information might be as crucial as the technological functioning of the app as such. Through our survey experiment, we investigate the information effect in more detail. We find support for a positive effect of providing additional information about the public health gains of the health authorities using personal data. On the other hand, contrary to our hypothesis, i.e., that providing information about the privacy cost will make people less positive about public use of personal data, we do not find a significant effect for this type of information. When comparing the effect of the two treatments, we do not find a significant difference between them. One potential mechanism behind these results could be that the mere act of emphasizing the privacy cost would make the perception of the situation around disease control even more serious. This could then lead to higher acceptance of strong and potentially intrusive measures. This potential mechanism should be the subject of future research. Overall, the

evidence from the literature is not straightforward. For example, experimental evidence from Marreiros et al. (2017) suggests that providing both negative and positive information about privacy decreases the propensity to disclose personal data, but has no effect on stated attitudes about privacy. Given these somewhat contradictory findings, more research is needed in order to gain a better understanding of the effect of information.

We also examine whether our findings are stable over time. During the first survey wave, the sense of urgency and uncertainty was most likely higher than during the second wave. We find that attitudes were quite stable across the two points in time. However, both waves were conducted during the COVID-19 pandemic and it would be interesting to analyze whether attitudes have changed after a much longer period, when the pandemic is over.

Finally, we compare attitudes to privacy in Norway and Sweden. It would not have been surprising if the more lenient approach taken by the Swedish government, compared to the measures implemented in Norway, had led to differences in privacy attitudes between the two countries. Especially when the first survey wave was conducted, the Swedish approach sent a signal that the pandemic could be handled without strict measures, and this approach could have made the population less willing to share data. Our results suggest that, contrary to what one might expect, attitudes are quite similar in the two countries. Overall, high trust in the authorities, and more positive preferences for collectivist approaches, may have played a bigger role than the policies implemented to control the spread of COVID-19. Both Norway and Sweden have high social trust and collectivist preferences. It would therefore be interesting to study similar attitudes in countries where trust and social responsibility are lower. In addition, this study has focused on describing privacy attitudes and potential changes, but it does not measure actual behavior or intentions. Consequently, future research should aim to investigate the link between stated attitudes and actual behavior as regards the public use of personal data.

## References

- Acquisti, A., L. Brandimarte, and G. Loewenstein (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology* 30(4), 736–758.
- Acquisti, A., S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati (2007). What can behavioral economics teach us about privacy? In *Digital privacy*, pp. 385–400. Auerbach Publications.

- Acquisti, A., C. Taylor, and L. Wagman (2016). The economics of privacy. *Journal of economic Literature* 54(2), 442–92.
- Alfnes, F. and O. C. Wasenden (2022). Your privacy for a discount? exploring the willingness to share personal data for personalized offers. *Telecommunications Policy* 46(7), 102308.
- Altmann, S., L. Milsom, H. Zillessen, R. Blasone, F. Gerdon, R. Bach, F. Kreuter, D. Nosenzo, S. Toussaert, and J. Abeler (2020). Acceptability of app-based contact tracing for covid-19: Cross-country survey study. *JMIR mHealth and uHealth* 8(8), e19857.
- Andersson, S. and N. Aylott (2020). Sweden and coronavirus: Unexceptional exceptionalism. *Social Sciences* 9(12), 232.
- Athey, S., C. Catalini, and C. Tucker (2017). The digital privacy paradox: Small money, small costs, small talk. Technical report, National Bureau of Economic Research.
- Bartling, B., A. Cappelen, H. Hermes, M. Skivenes, and B. Tungodden (2020). Free to fail? paternalistic preferences in the u.s. Technical report, mimeo NHH.
- Bartsch, M. and T. Dienlin (2016). Control your facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 56, 147–154.
- Baruh, L., E. Secinti, and Z. Cemalcilar (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67(1), 26–53.
- Benndorf, V. and H.-T. Normann (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics* 120(4), 1260–1278.
- Budd, J., B. S. Miller, E. M. Manning, V. Lampos, M. Zhuang, M. Edelstein, G. Rees, V. C. Emery, M. M. Stevens, N. Keegan, et al. (2020). Digital technologies in the public-health response to covid-19. *Nature medicine* 26(8), 1183–1192.
- Campos-Mercade, P., A. N. Meier, F. H. Schneider, and E. Wengström (2021). Prosociality predicts health behaviors during the covid-19 pandemic. *Journal of public economics* 195, 104367.
- Chan, E. Y. and N. U. Saqib (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when covid-19 concerns are high. *Computers in Human Behavior* 119, 106718.



- Christensen, T. and P. Lægreid (2020). Balancing governance capacity and legitimacy: how the norwegian government handled the covid-19 crisis as a high performer. *Public Administration Review* 80(5), 774–779.
- Dennis, S., S. Lewandowsky, P. Lorenz-Spreen, K. Oberauer, Y. Okan, R. Goldstone, Y. Cheng-Ta, Y. Kashima, A. Perfors, J. White, et al. (2020). Social licensing of privacy-encroaching policies to address the covid-19 pandemic. URL: <https://stephanlewandowsky.github.io/UKsocialLicence/index.html>.
- Dinev, T. and P. Hart (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research* 17(1), 61–80.
- European Data Protection Board (2020). Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the covid-19 outbreak.
- Evjemo, B., G. Gr, R. Ling, W. Nag, H. Röhr, and O. C. Wasenden (2020). Privacy on smartphones: A cross-national study. In *The Oxford Handbook of Mobile Communication and Society*. Oxford University Press.
- Fox, G., T. Clohessy, L. van der Werff, P. Rosati, and T. Lynn (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior* 121, 106806.
- Gómez-Barroso, J. L. (2018). Experiments on personal information disclosure: Past and future avenues. *Telematics and Informatics* 35(5), 1473–1490.
- Grossklags, J. and A. Acquisti (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In *WEIS*. Citeseer.
- Helsingen, L. M., E. Refsum, D. K. Gjøstein, M. Løberg, M. Bretthauer, M. Kalager, and L. Emilsson (2020). The covid-19 pandemic in norway and sweden—threats, trust, and impact on daily life: a comparative survey. *BMC public health* 20(1), 1–10.
- Julienne, H., C. Lavin, C. Belton, M. Barjaková, S. Timmons, and P. D. Lunn (2020). Behavioural pre-testing of covid tracker, ireland’s contact-tracing app.
- Kampmark, B. (2021). Covid meets volvo: The swedish public health approach to coronavirus. *Australian and New Zealand Journal of European Studies* 13(1).
- Kaya, E. K. (2020). Safety and privacy in the time of covid-19: Contact tracing applications.

- Keith, M. J., S. C. Thompson, J. Hale, P. B. Lowry, and C. Greer (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies* 71(12), 1163–1173.
- Kemp, S. (2021). Digital 2021: Global overview report — DataReportal— Global Digital Insights.
- Kobsa, A., H. Cho, and B. P. Knijnenburg (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An e laboration l ikelihood m odel approach. *Journal of the Association for Information Science and Technology* 67(11), 2587–2606.
- Li, T., C. Cobb, J. Yang, S. Baviskar, Y. Agarwal, B. Li, L. Bauer, and J. I. Hong (2021). What makes people install a covid-19 contact-tracing app? understanding the influence of app design and individual difference on contact-tracing app adoption intention. *Pervasive and Mobile Computing*, 101439.
- Marreiros, H., M. Tonin, M. Vlassopoulos, and M. Schraefel (2017). Now that you mention it”: A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization* 140, 1–17.
- Munzert, S., P. Selb, A. Gohdes, L. F. Stoetzer, and W. Lowe (2021). Tracking and promoting the usage of a covid-19 contact tracing app. *Nature Human Behaviour* 5(2), 247–255.
- Pape, S., D. Harborth, and J. L. Kröger (2021). Privacy concerns go hand in hand with lack of knowledge: The case of the german corona-warn-app. In *IFIP International Conference on ICT Systems Security and Privacy Protection*, pp. 256–269. Springer.
- Park, Y. J. and S. M. Jang (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior* 38, 296–303.
- Paterlini, M. (2020). Closing borders is ridiculous’: the epidemiologist behind sweden’s controversial coronavirus strategy. *Nature* 580(7805), 574.
- Rosenthal, S., O.-C. Wasenden, G.-A. Gronnevet, and R. Ling (2020). A tripartite model of trust in facebook: acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology* 23(6), 840–864.
- Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management* 55, 102178.

- Sandvik, K. B. (2020). “Smittestopp”: If you want your freedom back, download now. *Big Data & Society* 7(2), 2053951720939985.
- Sareen, S., K. B. Nielsen, P. Oskarsson, and D. Remme (2021). The pandemic as a rupture that follows rules: Comparing governance responses in india, usa, sweden and norway. Technical report.
- Simko, L., R. Calo, F. Roesner, and T. Kohno (2020). Covid-19 contact tracing and privacy: studying opinion and preferences. *arXiv preprint arXiv:2005.06056*.
- Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.* 126, 1880.
- Sweeney, Y. (2020). Tracking the debate on covid-19 surveillance tools. *Nature Machine Intelligence* 2(6), 301–304.
- Thomas, R., Z. A. Michaleff, H. Greenwood, E. Abukmail, and P. Glasziou (2020). Concerns and misconceptions about the australian government’s covidsafe app: cross-sectional survey study. *JMIR public health and surveillance* 6(4), e23081.
- Trang, S., M. Trenz, W. H. Weiger, M. Tarafdar, and C. M. Cheung (2020). One app to trace them all? examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems* 29(4), 415–428.
- Trepte, S., D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind (2015). Do people know about privacy and data protection strategies? towards the “online privacy literacy scale” (oplis). In *Reforming European data protection law*, pp. 333–365. Springer.
- Utz, C., S. Becker, T. Schnitzler, F. M. Farke, F. Herbert, L. Schaewitz, M. Degeling, and M. Dürmuth (2021). Apps against the spread: Privacy implications and user acceptance of covid-19-related smartphone apps on three continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–22.
- Vogel, G. (2020). Sweden’s gamble. *Science* 370(6513), 159–163.
- Yoo, B., N. Donthu, and T. Lenartowicz (2011). Measuring hofstede’s five dimensions of cultural values at the individual level: Development and validation of cvscafe. *Journal of international consumer marketing* 23(3-4), 193–210.

# Appendix

## A Additional tables

Table A.1: Background characteristics of the survey sample and official statistical data

Norway					
	Wave 1	Wave 1&2	N	<i>p</i> -value	Pop
Age	50	52	1387	0.000	
Female	0.50	0.50	1387	0.848	0.50
Higher education	0.61	0.60	1387	0.215	0.35
Employed	0.61	0.58	1387	0.000	0.58
Living alone	0.21	0.22	1387	0.100	0.18
Household income	1.99	1.97	1152	0.272	
Sweden					
Age	46	48	1200	0.000	
Female	0.51	0.50	1200	0.285	0.49
Higher education	0.61	0.61	1191	0.818	0.38
Employed	0.68	0.68	1194	0.826	0.68
Living alone	0.24	0.23	1200	0.340	0.19
Household income	1.91	1.92	1074	0.765	

*Notes:* The table lists background characteristics of the respondents in both Norway and Sweden. “Higher education” is an indicator taking value 1 if the respondent has a post-secondary education. “Employed” is an indicator taking value 1 if the respondent is in full or part-time employment. “Living alone” is an indicator taking value 1 if the respondent is living alone. “Household income” is a categorical variable taking value 1 if the respondent has a low income, 2 for a middle income and 3 for a high income. The first column reports averages for all respondents in the first wave (spring 2020), while the second column reports averages for the second wave (respondents who completed the survey in both spring and fall 2020). The third column reports the number of observations in the first wave. The fourth column reports the *p*-value of a t-test ( $\chi^2$  test for household income) between the respondents who completed only the first survey wave and those who completed both waves. The last column reports averages from Statistics Norway and Statistics Sweden, respectively. The shares from the official statistics have been calculated on the same age range as the sample (17-74 in Sweden and 18-88 in Norway), except for “Living alone”, which is calculated for the entire population.

Table A.2: Summary statistics - personal characteristics - Norway

	Spring 2020			Fall 2020			<i>p</i> -value
	Mean	St.Dev.	N	Mean	St.Dev.	N	
<i>Concern about privacy</i>							
Privacy concerned*	0.41	0.49	958	0.41	0.49	958	0.723
Collection of personal data	0.78	0.42	952	0.78	0.42	953	
Data used for other purposes	0.83	0.38	952	0.85	0.36	947	
Collection of too much information	0.74	0.44	952	0.73	0.45	955	
<i>Knowledge about privacy</i>							
Privacy knowledgeable*	0.48	0.50	958	0.49	0.50	958	0.173
Location registration	0.93	0.25	950	0.94	0.24	954	
Privacy notice	0.53	0.50	948	0.56	0.50	952	
Deletion of data	0.63	0.48	951	0.63	0.48	945	
GPS deactivation	0.60	0.49	948	0.64	0.48	954	
Browser history	0.82	0.38	952	0.84	0.37	953	
<i>Trust</i>							
Trust in health authorities*	0.87	0.33	951	0.83	0.37	946	0.589
Trust in politicians	0.40	0.49	949	0.30	0.46	949	
Trust in research institutes	0.69	0.46	930	0.70	0.46	935	
<i>Collectivist preferences</i>							
Collectivist*	0.49	0.50	958	0.53	0.50	958	0.771
Restrict personal freedom	0.47	0.50	946	0.38	0.49	952	
People make bad choices	0.62	0.49	943	0.61	0.49	955	
Sacrifice self-interest	0.45	0.50	945	0.36	0.48	947	
Group goals first	0.42	0.49	949	0.35	0.48	948	

*Notes:* The table lists the average shares of respondents expressing agreement for all variables relating to privacy concern and knowledge, trust levels, and collectivist preferences. Variables with an asterisk are the variables used in the main analyses. *Privacy concerned* is an indicator variable taking value 1 if the respondents have a value for the concern index higher than the average in their sample group. *Collectivist* is defined in a similar way. *Trust in health authorities* is an indicator variable taking value 1 if the respondents answer agree or strongly agree to the question asked. *Privacy knowledgeable* is an indicator variable taking value 1 if the respondents have answered all five questions (almost) correctly. The other variables for *Concern about privacy*, *Trust*, and *Collectivist preferences* are defined as indicator variables taking value 1 if the respondents answer agree or strongly agree to the question asked. The other variables for *Knowledge about privacy* report the share of respondents who answered the question (almost) correctly. The last column reports the *p*-value of a t-test between respondents who only completed the first survey wave and those who completed both waves for the variables used in the main analysis.

Table A.3: Summary statistics - personal characteristics - Sweden

	Spring 2020			Fall 2020			<i>p</i> -value
	Mean	St.Dev.	N	Mean	St.Dev.	N	
<i>Concern about privacy</i>							
Privacy concerned*	0.46	0.50	945	0.51	0.50	945	0.214
Collection of personal data	0.79	0.41	941	0.84	0.37	941	
Data used for other purposes	0.90	0.29	943	0.92	0.27	942	
Collection of too much information	0.70	0.46	943	0.74	0.44	940	
<i>Knowledge about privacy</i>							
Privacy knowledgeable*	0.54	0.50	945	0.56	0.50	945	0.908
Location registration	0.95	0.22	944	0.95	0.22	942	
Privacy notice	0.53	0.50	943	0.56	0.50	941	
Deletion of data	0.65	0.48	942	0.68	0.47	943	
GPS deactivation	0.71	0.45	942	0.73	0.44	942	
Browser history	0.88	0.33	944	0.89	0.32	941	
<i>Trust</i>							
Trust in health authorities*	0.84	0.36	938	0.79	0.41	934	0.585
Trust in politicians	0.39	0.49	939	0.28	0.45	943	
Trust in research institutes	0.77	0.42	934	0.76	0.43	929	
<i>Collectivist preferences</i>							
Collectivist*	0.54	0.50	945	0.49	0.50	945	0.861
Restrict personal freedom	0.39	0.49	942	0.32	0.47	941	
People make bad choices	0.41	0.49	941	0.36	0.48	942	
Sacrifice self-interest	0.34	0.47	941	0.24	0.43	940	
Groups goals first	0.26	0.44	937	0.24	0.43	938	

*Notes:* The table lists the average shares expressing agreement for all variables relating to privacy concern and knowledge, trust levels, and collectivist preferences. Variables with an asterisk are the variables used in the main analyses. *Privacy concerned* is an indicator variable taking value 1 if the respondents have a value for the concern index larger than the average in their sample group. *Collectivist* is defined in a similar way. *Trust in health authorities* is an indicator variable taking value 1 if the respondents answer agree or strongly agree to the question asked. *Privacy knowledgeable* is an indicator variable taking value 1 if the respondents have answered all five questions (almost) correctly. The other variables for *Concern for privacy*, *Trust* and *Collectivist preferences* are defined as indicator variables taking value 1 if the respondents answer agree or strongly agree to the question asked. The other variables for *Knowledge about privacy* report the share of respondents who answered the question (almost) correctly. The last column reports the *p*-value of a t-test between respondents who completed only the first survey wave and those who completed both waves for the variables used in the main analysis.

Table A.4: Balance test by treatment

	Norway				Sweden			
	Control	Privacy cost	Public health gain	$p$ -value	Control	Privacy cost	Public health gain	$p$ -value
Age	52	53	52	0.823	48	48	49	0.651
Female	0.49	0.53	0.49	0.605	0.51	0.49	0.50	0.869
Higher education	0.58	0.60	0.62	0.671 (0.150)	0.57	0.60	0.66	0.084 (0.258)
Employed	0.58	0.56	0.58	0.834 (0.836)	0.70	0.63	0.69	0.110 (0.170)
Living alone	0.24	0.20	0.21	0.446 (0.848)	0.24	0.18	0.26	0.045 (0.304)
Household income	1.94	2.01	1.97	0.892 (0.547)	1.84	1.96	1.95	0.245 (0.711)

*Notes:* The table reports average values for background information on the respondents in both Norway and Sweden across the control group and the two information treatments. Descriptions of the variables are available in the notes to Table A.1. The last columns in each panel report the  $p$ -value of Pearson's chi-squared test for categorical variables (female and household income) and the  $p$ -value of the Kruskal-Wallis rank test with tied data for all other variables. In parenthesis, the  $p$ -value of the Pearson's chi-squared test is reported for the full categorical variables related to education, employment status, living conditions, and income.

Table A.5: Summary statistics - public use of personal data with pooled data, spring 2020

	Mean	St.Dev	N
Gather anonymous location data	0.72	0.45	2581
Track movements	0.54	0.50	2564
Text warning of infections	0.81	0.39	2572
Text with quarantine warning	0.73	0.45	2571
App to track location	0.47	0.50	2567
App to track location and health	0.42	0.49	2564
App for location, health and contact tracing	0.60	0.49	2556
Privacy attitude index	0.45	5.75	2587

*Notes:* The table lists summary statistics for all variables relating to attitudes to the use of personal data by the health authorities. The variables are defined as indicator variables that take value 1 if the respondents agree or strongly agrees with the use of personal data. *Privacy attitude index* is constructed by summing the standardized version of the seven variables.



Table A.6: Summary statistics - public use of personal data

	Spring 2020			Fall 2020			
Panel A - Norway							
	Mean	St.Dev.	N	Mean	St.Dev.	N	<i>p</i> -value
Gather anonymous location data	0.72	0.45	955	0.69	0.46	952	0.488
Track movements	0.50	0.50	946	0.50	0.50	947	0.446
Text warning of infections	0.81	0.39	949	0.78	0.41	950	0.692
Text with quarantine warning	0.79	0.41	952	0.78	0.41	944	0.103
App to track location	0.48	0.50	945	0.47	0.50	946	0.857
App to track location and health	0.42	0.49	944	0.36	0.48	948	0.470
App for location, health and contact tracing	0.60	0.49	947	0.56	0.50	947	0.127
Privacy attitude index	0.45	5.77	958	0.47	5.93	958	0.944
Panel B - Sweden							
Gather anonymous location data	0.73	0.44	943	0.67	0.47	941	0.940
Track movements	0.60	0.49	940	0.54	0.50	941	0.092
Text warning of infections	0.82	0.38	940	0.78	0.42	944	0.461
Text with quarantine warning	0.68	0.47	939	0.63	0.48	945	0.233
App to track location	0.45	0.50	942	0.48	0.50	940	0.772
App to track location and health	0.41	0.49	939	0.41	0.49	939	0.774
App for location, health and contact tracing	0.58	0.49	935	0.56	0.50	930	0.937
Privacy attitude index	0.50	5.82	945	0.50	6.00	945	0.270

*Notes:* The table lists summary statistics for all variables relating to attitudes to the use of personal data by the health authorities. The variables are defined as indicator variables that take value 1 if the respondents agree or strongly agree with the use of personal data. The *Privacy attitude index* is constructed by summing the standardized version of the seven variables. Panel (a) reports statistics from the Norwegian sample, while panel (b) reports statistics from the Swedish sample. The last column reports the *p*-values for equal means between respondents who only completed the first survey wave and those who completed both waves, using a Mann-Whitney test for the Privacy attitude index and t-test for the other variables.

Table A.7: Regression of personal characteristics on personal data usage

Dep. var.:	Norway and Sweden
Privacy attitude index	Spring 2020
Privacy concerned	-2.392*** (0.243)
Privacy knowledgeable	-0.144 (0.244)
Trust in health authorities	2.038*** (0.376)
Collectivist	2.322*** (0.233)
Age	0.027*** (0.007)
Female	0.602** (0.234)
Higher education	-0.663*** (0.241)
Employed	-0.572** (0.276)
Living alone	-0.389 (0.326)
Middle Income	0.321 (0.312)
Higher income	0.898** (0.367)
Constant	-2.422*** (0.653)
Observations	2206
Adjusted $R^2$	0.120

*Notes:* The table reports OLS coefficients of regressing personal characteristics (privacy concerned, privacy knowledgeable, trust in the health authorities, collectivist preferences) on the “Privacy attitude index” of the seven standardized variables on the use of personal data, for all respondents in the first survey wave. Figure 2 visualizes the same regression. Descriptions of the variables for the personal characteristics are available in the notes to Table A.2. A set of demographic controls is included in the regression. Standard errors are in parenthesis. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

Table A.8: Difference between the two information treatments as regards privacy attitudes

Dep. var.:	Norway and Sweden		
	Spring 2020		
Privacy attitude index			
Public health gain	0.279 (0.274)	0.185 (0.263)	0.281 (0.282)
Privacy concerned		-2.088*** (0.278)	-2.124*** (0.299)
Privacy knowledgeable		-0.472 (0.264)	-0.133 (0.295)
Trust in health authorities		2.016*** (0.442)	1.652*** (0.466)
Collectivist		2.246*** (0.264)	2.346*** (0.285)
Age			0.036*** (0.009)
Female			0.225 (0.283)
Higher education			-0.456 (0.287)
Employed			-0.277 (0.336)
Living alone			-0.472 (0.403)
Middle income			0.265 (0.382)
High income			0.710 (0.451)
Constant	0.536** (0.191)	-1.202* (0.486)	-2.620** (0.830)
Observations	1733	1723	1480
Adjusted $R^2$	0.000	0.095	0.104

*Notes:* The table reports OLS coefficients of regressing the two information treatments, excluding the control group, on the *Privacy attitude index* for the full sample combining Norway and Sweden in the first wave. The “Public health gains” coefficient is in this case compared to “Privacy cost”, to see whether the two treatments have different effects. Standard errors are in parenthesis. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

Table A.9: Regression of personal characteristics on personal data usage by country and survey wave

Dep. var.:	Norway		Sweden	
Privacy attitude index	Spring 2020	Fall 2020	Spring 2020	Fall 2020
Privacy concerned	-2.803*** (0.408)	-2.176*** (0.412)	-2.308*** (0.403)	-2.012*** (0.400)
Privacy knowledgeable	-0.636 (0.402)	-0.390 (0.418)	-0.224 (0.401)	-0.486 (0.412)
Trust in health authorities	2.717*** (0.626)	4.324*** (0.624)	1.132* (0.589)	2.075*** (0.535)
Collectivist	2.374*** (0.380)	2.686*** (0.400)	2.288*** (0.400)	2.505*** (0.394)
Demographic controls	✓	✓	✓	✓
Observations	794	789	834	828
Adjusted $R^2$	0.190	0.193	0.095	0.111

*Notes:* The table reports OLS coefficients of jointly regressing personal characteristics on the index of the seven standardized variables relating to the use of personal data, for all four samples (both waves in each country). Descriptions of the variables for personal characteristics are available in the notes to Table A.2. A set of demographic controls is included in the regression. Standard errors are in parenthesis. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

Table A.10: Survey experiment and time difference

Dep. var:	Pooled data	Pooled data	Pooled data
Privacy attitude index	Spring 2020	Fall 2020	Both waves
Privacy costs	0.438 (0.281)	0.464 (0.336)	0.455 (0.281)
Public health gain	0.724* (0.285)	0.796* (0.339)	0.732* (0.285)
Control $\times$ Fall 2020			0.088 (0.310)
Privacy costs $\times$ Fall 2020			0.106 (0.306)
Health benefits $\times$ Fall 2020			0.174 (0.317)
Personal characteristics	✓	✓	✓
Demographic controls	✓	✓	✓
Constant	-2.849*** (0.684)	-5.117*** (0.821)	-3.837*** (0.537)
Observations	2206	1617	3823
Adjusted $R^2$	0.122	0.145	0.132

*Notes:* The table reports OLS coefficients of regressing the two information treatments, (categorical variable with “Control” as the reference category and “Privacy cost” and “Public health gains” reported in the table) on the *Privacy attitude index* for the full sample combining Norway and Sweden in the first wave, then the second wave and finally, pooled over the two countries and the two waves. In the third regression, we include the interactions between the treatments and the survey wave. We also include personal characteristics as described in the notes to Table 2 and a set of demographic controls. Standard errors are in parentheses. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

Table A.11: The effects of information provision on privacy attitudes by country and by survey wave

Dep. var.	Norway		Sweden	
	Spring 2020	Fall 2020	Spring 2020	Fall 2020
Privacy cost	0.800* (0.464)	0.779 (0.473)	0.322 (0.462)	0.252 (0.481)
Public health gain	0.681 (0.452)	0.559 (0.471)	0.978** (0.484)	1.027** (0.485)
Privacy concerned	-2.790*** (0.407)	-2.182*** (0.412)	-2.273*** (0.403)	-2.011*** (0.399)
Privacy knowledgeable	-0.597 (0.400)	-0.324 (0.419)	-0.222 (0.400)	-0.482 (0.410)
Trust in health authorities	2.670*** (0.626)	4.301*** (0.627)	1.183** (0.586)	2.041*** (0.532)
Collectivist	2.362*** (0.381)	2.664*** (0.401)	2.270*** (0.400)	2.514*** (0.396)
Constant	-4.347*** (1.229)	-5.551*** (1.211)	-0.863 (1.161)	-5.072*** (1.134)
Observations	794	789	834	828
Adjusted $R^2$	0.192	0.194	0.098	0.114

*Notes:* The table reports OLS coefficients of regressing the two information treatments (categorical variable with “Control” as the reference category, and “Privacy cost” and “Public health gains” reported in the table) on the *Privacy attitude index*, for all four samples (both waves in each country). Descriptions of the variables for the personal characteristics are available in the notes to Table A.2. A set of demographics controls is included in the regression. Standard errors are reported in parentheses. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

## B More details on the sample

The surveys were conducted in collaboration with the global market research agency Kantar in April 2020 and October-November 2020 in both Norway and Sweden.<sup>12</sup> In the first wave, we asked respondents whether they were willing to be contacted again at a later stage. Only respondents who agreed to be re-contacted were included in the survey in the first wave. The questions in the second wave were exactly the same as those used in April. In Norway, 1387 respondents completed the first wave and 958 completed both waves of the surveys. In Sweden, 1200 respondents completed the first, while 945 completed both waves. Attrition was not random, but it did not affect responses to the survey questions. Among those completing the first wave but not the second, there were more younger respondents in both Norway and Sweden and more employed individuals in Norway compared to subjects completing both waves (see Table A.1 for more details). Importantly, the shares in both samples are comparable to the national averages (see the last column in Table A.1). The samples in both countries are quite representative of the working population, with a bias towards respondents with higher education. There are no significant differences between respondents completing only the first wave and those completing both waves for all other questions in the survey (see the last column in Tables A.2, A.3 and A.6 for details.)

## C More details on attitudes to privacy, trust and collectivist preferences

In the first part of the survey, respondents answered questions about different dimensions that could affect their willingness to share personal data. In particular, we included measures for privacy concern, privacy knowledge, and trust in relevant agencies. In addition, given the context of using individuals' personal data for a social purpose, we asked questions about respondents' attitudes to government interventions and individual self-sacrifice.

**Privacy concern and knowledge.** The instruments for privacy concern and privacy knowledge are mainly based on Park and Jang (2014), Trepte et al. (2015), and Kobsa et al. (2016), and they have been used earlier in Evjemo et al. (2020) and Alfnes and Wasenden (2022). For privacy concern, respondents were asked to state on a 5-point Likert scale the extent to which they agreed with statements regarding the collection and use of personal data. Details

---

<sup>12</sup>In Norway, the first survey ran from April 6 to April 20, and the second wave ran from October 20 to November 11. In Sweden, the first survey ran from April 8 to April 17, and the second wave from October 15 to November 10.

of the items can be found in the Appendix Section D. Tables A.2 and A.3 report summary statistics for the average share of respondents expressing agreement with these statements for both survey waves in Norway and Sweden, respectively. For each statement, we find quite high shares agreeing with concern issues in both Norway and Sweden (on average across all three statements, 78% of the respondents in Norway and 80% in Sweden agree or strongly agree). We find no large differences across the two survey waves in Norway, while we find significantly higher concern levels in Sweden in fall 2020 compared to six months earlier.<sup>13</sup> Based on the three statements, we construct an index by summing the standardized version of the variables. The Cronbach’s alpha for the index is between 0.79 and 0.81 across the four samples (two survey waves in Norway and two in Sweden), indicating strong internal consistency. We then define a respondent as being privacy concerned if the value for the index is above the average (for each wave and country). On average, we found that 41% of the Norwegian sample were privacy concerned in both survey waves, while we find slightly larger shares for Sweden (46% in spring 2020 and 51% in fall 2020).

With respect to privacy knowledge, respondents had to guess whether five statements about the handling of personal data were true or false. The answer scale ranged from “Definitely true” and “Probably true” to “Probably false” and “Definitely false”, and included an “I do not know” option. Three out of the five statements were true, while the other two were false. Details of the specific items can be found in the Appendix section D, and summary statistics for the shares of respondents who answered each statement (almost) correctly are reported in Tables A.2 and A.3. On average across the five statements, 70% of the respondents in Norway and 74% in Sweden (almost) had the right answers. We find no large differences in privacy knowledge across the two survey waves in both countries.<sup>14</sup> We define a respondent to be privacy knowledgeable if he/she on average guesses almost correctly the answer to all five questions.<sup>15</sup> About half of respondents in Norway have some knowledge about privacy (48% in spring 2020 and 49% in fall 2020). Like privacy concern, we find slightly larger shares for privacy knowledge in Sweden (54% in spring 2020 and 56% in fall 2020). For both privacy concern and knowledge, the descriptive results are in line with previous studies that have used similar measures (Evjemo et al., 2020; Alfnes and Wasenden, 2022). In line with these studies, we expected respondents who are privacy concerned and privacy

<sup>13</sup>The  $p$ -values from a Mann-Whitney test of the full categorical variable of the three statements are  $p < 0.05$ ,  $p < 0.00$  and  $p < 0.01$ , respectively.

<sup>14</sup>In Norway, for the statement on GPS deactivation, more respondents answered correctly ( $p < 0.1$ ), while in Sweden, for the statement on deletion of data, more respondents answered correctly ( $p < 0.1$ ).

<sup>15</sup>We define a score from 0 to 4 for each statement, where 0 is assigned to the completely wrong answer (e.g., “Definitely false” for a true statement) and 4 is assigned to the completely correct answer. Summing the scores over the five statements, the maximum score is 20 and we define the respondent to be privacy knowledgeable if his/her score is equal to or above 15.



knowledgeable to be less positive about the use of personal data by the health authorities.

**Trust.** After the questions about privacy, respondents were asked (on a 5-point Likert scale) whether they found health authorities, politicians and research institutes to be trustworthy.<sup>16</sup> As shown in Tables A.2 and A.3, trust levels in health authorities are very high in both countries (87% in Norway and 84% in Sweden) in the first survey wave, but respondents reported lower trust, 4(5) percentage points lower in Norway(Sweden) in the second survey wave ( $p < 0.01$  in Norway and  $p < 0.01$  in Sweden base on a Mann-Whitney test of the full categorical variable). A larger decline in trust in fall 2020 compared to six months earlier is also found for trust in politicians ( $p < 0.00$  in both countries). Increasing distrust in public and political entities could be influenced by the approaches taken by the governments in both countries (add reference and rephrase!). Instead, we find constant high levels of trust in research institutes (69% in Norway and 77% in Sweden) across both survey waves. We expected trust, especially in the health authorities, to have a positive relationship with attitudes to the use of personal data.

**Collectivist preferences.** Finally, we asked two questions about preferences for paternalistic interventions, inspired by Bartling et al. (2020), and two questions about collectivist approaches, inspired by Yoo et al. (2011). Respondents were asked on a 5-point Likert scale to state the extent to which they agreed with four statements about these topics. Details on the specific items can be found in the Appendix section D, and summary statistics for the average share expressing agreement with these statements are reported in Tables A.2 and A.3. First, we observe certain differences across the two countries. On average across the four statements, the shares expressing agreement with statements on these topics are 49% in Norway and 35% in Sweden. Secondly, we find lower collectivist preferences across almost all four statements in fall 2020 compared to spring 2020 in both countries.<sup>17</sup> Based on the four statements, we construct an index for collectivist preferences by summing the standardized version of variables. The Cronbach's alpha for the index is between 0.77 and 0.81 across the four samples (two waves in Norway and Sweden), indicating strong internal consistency. We define a respondent to have collectivist (versus individualistic) preferences if the value of the index is above the average (for each wave and country). Interestingly, we find higher shares of collectivists in Sweden in the first survey wave (54% in Sweden vs. 49% in Norway), but

---

<sup>16</sup>We also asked about the level of trust in other companies, such as cell phone operators, Facebook, Google, Apple, and Samsung, but we excluded these questions from the analyses, as they are not the focus of this study.

<sup>17</sup>The  $p$ -values from a Mann-Whitney test of the full categorical variable of the four statements are  $p < 0.00$ ,  $p > 0.1$ ,  $p < 0.00$ ,  $p < 0.00$  in Norway and  $p < 0.00$ ,  $p < 0.05$ ,  $p < 0.00$ ,  $p > 0.1$  in Sweden.

the opposite in the second survey wave, when a larger share of Norwegian respondents agree with collectivist statements than in Sweden (53% in Norway vs. 49% in Sweden).<sup>18</sup> We expected these collectivist preferences to have a positive relationship with attitudes to the use of personal data, given that the data are used for a public cause.

---

<sup>18</sup>The differences are significant between the two countries for both survey waves ( $p = 0.029$  in spring 2020 and  $p = 0.071$  in fall 2020 from a Student-t test) and between the two survey waves for both countries ( $p = 0.091$  in Norway and  $p = 0.021$  in Sweden based on a Student-t test).

## D Survey questions

1. The purpose of this survey is to understand your attitudes to topics such as trust and privacy, and your willingness to share personal data with the health authorities in a crisis situation. The survey will be repeated at a later date, and we are therefore dependent on you answering in the next survey as well. Is that okay with you?
2. We will first ask you questions related to personal data when using the Internet.
3. Do you agree or disagree with the following statements? (Answer scale: strongly disagree to strongly agree.)
  - It usually bothers me when cell phone applications ask me for personal information
  - It bothers me that personal information given to online companies for a specific purpose can be used for other purposes
  - I am concerned that online companies are collecting too much personal information about me
4. Based on your knowledge, are the following statements true or not? (Answer scale: definitely true, probably true, I don't know, probably false, definitely false)
  - Many cell phone apps record your location
  - When a cell phone app has a privacy policy, this means that no personal data are shared with other apps or companies
  - Facebook, Google, and similar companies delete personal data after a predefined period
  - When you deactivate GPS on your phone, your location cannot be tracked
  - Your browsing history is normally stored on your cell phone
5. You will now be asked some questions related to trust.
6. Generally speaking, would you say that most people can be trusted, or that you need to be very careful when dealing with people? (Answer scale: Most people can be trusted to You need to be very careful)
7. Do you agree or disagree that these companies/agencies are trustworthy? (Answer scale: strongly disagree to strongly agree + Not relevant/Don't know the company)
  - Your cell phone operator

- Facebook
- Google
- Apple
- Samsung
- Health authorities
- Norwegian politicians
- Research institutions

8. In the following, we will ask your opinion on statements related to individual freedom. There are no right or wrong answers – just give your honest opinion.

9. Please indicate the extent to which you agree or disagree with each statement. (Answer scale: strongly disagree to strongly agree)

- The government should restrict people’s freedom to make certain choices if doing so would make people’s lives better
- People often make bad choices because they do not know what is best for them
- Individuals should sacrifice self-interest for the group
- Individuals should only pursue their goals after considering the welfare of the group

#### 10. COMMON INTRO TEXT FOR ALL THREE GROUPS

Read this text carefully before proceeding.

Think of a situation where health authorities want to use information about where people are and how they move around, so-called location data, to fight a serious infectious disease. Personal data will be handled in accordance with applicable laws and regulations. Location data can be collected using two different cell phone technologies.

- cell phones connect to base stations. Hence, information about your approximate location can be gathered from the cell phone network
- A smartphone app can use the GPS functionality to track your exact location

The health authorities can use either of these technologies to gain access to location data. The data can be used in ways that make you identifiable or they can be anonymized. In the latter case, it will, for example, be known how many people are in an area, but not who the individuals are.

11. PRIVATE COST INFORMATION

Mapping individuals' location in public places will come at the expense of privacy. Where a person is located is regarded as sensitive private information and the right to privacy is part of human rights.

12. PUBLIC HEALTH GAIN INFORMATION

Details about where people are, how they move around and who they are in contact with, are necessary in order to be able to efficiently combat an outbreak of a serious contagious disease. If the health authorities are able to gather and use such data efficiently, lives will be saved.

13. Given a situation like the one described above, consider the following questions:

14. During an outbreak of a serious contagious disease, how positive or negative would you rate it if the health authorities were to do the following? (Answer scale: very negative to very positive)

- ...gather anonymous data on people's location
- ...track your movements
- ...launch a cell phone app that tracks your location
- ...launch a cell phone app that tracks your location and your health status
- ...launch a cell phone app that tracks your location and your health status, and uses it to warn you if you have been in contact with people who are infected
- ...alert people in quarantine if they break the rules, and remind them of the potential consequences, through a text message
- ...ask you to leave an area due to a higher risk of infection, through a text message

15. The health authorities need large amounts of data to carry out the efficient and reliable analyses that are required to combat a serious contagious disease. For the authorities to get enough data through an app, it is necessary that a large share of the population uses the app. Given the need for many users, how positive or negative would you rate it if the health authorities were to do the following? (Answer scale: very negative to very positive)

- .... launch a cell phone app, **voluntary to have and use**, that tracks all the data needed to efficiently combat a serious contagious disease

- . . . launch a cell phone app, mandatory **to have and that cannot be deactivated**, that tracks all the data needed to efficiently combat a serious contagious disease
16. In general, how positive or negative would you rate it if your cell phone operator were to do the following? (Answer scale: very negative to very positive)
- . . . use your anonymized location data to understand how the population moves around
  - . . . share anonymous data on the cell phone users' location and movements with the health authorities
17. Which cell phone operator do you use?
18. Finally - some demographic questions.
19. Are you? Male, Female
20. What is your age?
21. What is your highest completed education level?
22. What is your main occupation?
23. Who do you live with?
24. What is your total household income before taxes?

## **Paper 4**





# Information Avoidance and Privacy — the role of Entertaining Content

Ceren Ay, Eleonora Freddi, and Ole Christian Wasenden

“Dude, no one reads the consent forms”

Anonymous participant in experiment

## Abstract

In this study, we investigate whether people are more likely to avoid information about privacy when they are exposed to highly entertaining online content. The idea is that consuming such content leads to high levels of hedonic well-being, and that such information is more likely to have a negative effect. To explore this, we conducted an experiment in which participants were shown videos online and asked to either seek out or avoid information about privacy. The entertainment value of the videos and the indicated time cost of obtaining the privacy information varied. We found that the entertainment value of the videos and the time cost had weak effects on information seeking. In addition, we found that participants who were exposed to entertaining content anticipated a more negative impact of privacy information on their user experience. Our results provide new insights into the role of hedonic well-being in privacy decisions and information avoidance, and they pave the way for further research on privacy decisions.

**Keywords:** Privacy, Economics, Attitude, Behavior, Information Avoidance

## 1 Introduction

In this study, we investigate the link from entertaining content, via hedonic well-being, to potential privacy information avoidance. We test whether someone exposed to highly entertaining

online content is more likely to avoid privacy information than someone exposed to less entertaining content. Sharot and Sunstein (2020) present a model in which disutility as a result of a potential reduction in hedonic well-being could be a reason to avoid information. Their model presents a general framework for information avoidance, and we study the topic in a specific privacy context. Privacy information could typically concern an online company's privacy policy, what personal data will be collected, and how the personal data will be handled, or a website's cookie settings.

Modern digital life comes with extensive trade in personal information, both between individuals and commercial actors, and between data-collecting firms and third parties such as advertisers (Bergemann et al., 2022). When an individual uses services from companies like Facebook and Google, the content will normally be personalized based on detailed information. This information, based on earlier online activities, could, for instance, be about age, gender, interests, where one lives, the device that is used, other devices used by the same individual, the social network, or data about others with a similar profile. Following Hoofnagle and Whittington (2013), companies like Facebook and Google base large parts of their business model on their end users' personal data. They market their services as free for end users, while what can be regarded as a hidden price is collected through personal data. The companies then monetise this information, for example through personalized advertisements.

Such data-collecting behavior is widespread among online firms and not limited to large companies. Consequently, users of digital services must frequently make choices about whether to share information about themselves when online. Normally the three main options are either to accept the default privacy settings and start using the service directly, to not use the service at all, or to seek more information and potentially change the privacy settings before using the service. This decision-making process, whether to seek more information or not, is what we investigate in this study. The relevant privacy information will normally be available by accessing a *consent page* or a *terms and conditions page* from the relevant service provider. According to classical economic theory, the privacy information would be beneficial. When making a decision, in this case whether or not to use a service, having more information would help individuals to make better decisions (Stigler, 1961). Consumers should benefit from having as much information as possible, also about privacy and the use of personal data, when deciding what services to use. Despite this, also in situations where the cost of reading the privacy information and, if neces-

sary, changing settings is low, users frequently make choices without accessing the information, contrary to what the classical model predicts.

The key element we investigate in this study is the level of entertainment of online content and the potential effects this can have on privacy information decisions. People might behave differently when they are entertained compared to a situation in which they, for example, are informed. The consumption of entertaining media content could potentially motivate individuals to avoid privacy information, because it could reduce their hedonic well-being, following Sharot and Sunstein (2020). There is also a well-established link in the literature between media entertainment and well-being, as described by Rieger et al. (2014).

Against this background, we formulate a main research question; *“Are people less likely to seek out privacy information when consuming more entertaining content compared to less entertaining content?”*. In addition, we formulate a secondary questions related to the time cost of seeking information; *“Does the time cost of obtaining information affect the likelihood of seeking the privacy information?”*. To answer our questions, we ran an experiment online on the crowdsourcing platform Prolific Academic, with participants from the USA and Canada. The participants were asked to watch and rate two videos produced by the multinational telecommunication provider Telenor. They were randomized in two groups, one group watching highly entertaining and the other group less entertaining, more informative videos. The videos were selected after a pre-test, which was also run on Prolific, where multiple videos were rated for their level of entertainment. The two most and the two least entertaining ones were used in the experiment. The participants were also randomly given different information about how much time it would take to obtain the privacy information before deciding whether or not to read a privacy notice.

In the experiment, the participants were shown a privacy pop-up before the first video, stating that personal data would be handled as described in the general consent form they had read when consenting to take part in the study. Then, at the beginning of the second video, a new privacy pop-up appeared, and the participants were told that the privacy settings for this second video might be different from those for the first one. They could then choose to either access the privacy information or move directly to watching the second video without reading the information. In the privacy notice, we included a treatment variation in the time cost, by indicating the difference in how much time it would take to read the notice, either 10 or 30 seconds. The key measurements in our experiment concern whether or not participants decide to access the

privacy information. In addition, we asked the respondents to state how large a share of the other participants they believed had been highly entertained when watching the first video. They had to base this belief on their own experience while watching the video, and this serves as an alternative measure of entertainment. We also measure the time the participants spend on the different steps throughout the experiment, making it possible to explore any variations in decision time across treatments. We also include common measures from the privacy literature, such as privacy concern and trust.

Our results show a tendency for participants exposed to more entertaining content and a higher reading time to be less likely to read the privacy notice. When testing the two treatments, we find significantly fewer readers among those exposed to long reading time, but no effect for the content treatment. However, when substituting the content treatment with secondary beliefs about entertainment levels, we also partly find a significantly lower share of readers based on the level of entertainment. When examining our results in more depth, we find other interesting patterns. The participants were asked whether they expected their user experience to be affected by the privacy information. The share expecting a negative impact was larger among those in the entertaining treatment group. Furthermore, looking at how much time the participants spend on deciding whether to read the privacy information, we find that it is significantly shorter among those who watched entertaining videos. Our findings indicate that the type of content and the time cost could play a role when people have to choose whether to access or avoid privacy information, but more research is needed to thoroughly understand this potential relationship.

The rest of the paper is organized as follows. In section 2, we review relevant literature. Then, in section 3, we formulate our hypothesis and our measurements. Sections 4 and 5 present our experimental design, our sample, and procedures. Our results are presented in section 6, and we set out some conclusions in section 7.

## **2 Literature**

Our results contribute to various strands of the literature on information preferences, privacy decisions, and the effects of hedonic utility on economic decisions. One key new element in our study is the possible effect of different levels of entertainment in digital media consumption. Stigler's (1961) seminal paper *The economics of information* is a cornerstone in the classical

economic theory of information. It emphasizes that, for rational actors, more information will always be positive, and it will help individuals make better decisions. Not accessing available information will only happen when the cost of collecting it is expected to be higher than the value of the information. Time will typically be considered as a transaction cost (DeSerpa, 1971). In many situations, however, the utility of acquiring information may be smaller than the disutility of doing so. One of the best known cases from the digital privacy area concerns cookie settings. Most of us will not always access the settings to learn about the details and perhaps adjust the cookie settings, but instead just click the accept button (Utz et al., 2019).

More recently, the idea that receiving information results in disutility has fed the growing literature on information avoidance. Information avoidance deviates from and extends the classical theories of information by introducing deliberate actions to avoid learning certain things when they are at odds with other benefits or temptations. Sweeny et al. (2010) define this as *any behavior designed to prevent or delay the acquisition of available but potentially unwanted information*. Golman et al. (2017) offer an alternative definition: *information avoidance as the deliberate decision not to learn when first, the decision maker is aware that the information is available and, second, the information is free to access*. One example they give concerns leaders avoiding learning information that is in conflict with their previous decisions, even when learning could help them not to implement decisions with potentially negative consequences.

Sharot and Sunstein (2020), present a framework model for how people decide to access or avoid information, when there is a trade-off between a positive and a negative impact on people's welfare. The value of information comes through either *action*, *affect*, or *cognition*. *Action*, the instrumental value, is information that makes it possible to make good decisions, following Stigler (1961). This is typically information that will enable the individual to achieve a goal. Normally this type of information would be positive. *Affect* is the hedonic value of information, i.e., the amount of positive feelings subtracted from the amount of negative feelings stemming from the information. If the latter dominate, the individual would be better off remaining ignorant. Lastly, *cognition*, is a type of information that will strengthen inner mental models. Simply knowing things could make you feel better, even when the knowledge is not utilized. In our study, we define information avoidance as not reading the privacy information that is made available to the participants. There could be several reasons for not reading it. In our experiment, we test time cost, which, according to the classical economic theory of information is a cost element that the

individual will consider. Time cost is a part of the *action* element in Sharot and Sunstein (2020), while the level of entertainment would fit with their *affect* element.

Sunstein (2019) provides evidence of information avoidance in the case of food labeling containing nutritional facts about a product. On the one hand, receiving such information can help people to make better choices for their health. On the other, such information might yield some disutility, while enjoying a tasty but calorific meal. In such cases, when deciding what to consume, people could decide to avoid information (Loewenstein and O'Donoghue, 2006; Sunstein, 2019). This potential behavior would be in line with the hedonic value logic of the model by Sharot and Sunstein (2020). Reisch et al. (2021) also focus on food labelling, and conclude that policymakers should also consider the hedonic effects of information when formulating food policy.

Svirsky (2022) studies information avoidance and privacy behavior. In an experiment, all participants were informed that they could take a survey either anonymously or after logging in with their Facebook account, with a privacy cost at the beginning. Giving up privacy would yield a higher payment, so there was a privacy for money trade-off. When making the actual choice, half of the sample received information about both privacy and payment levels, while, for the other group, the privacy information was hidden behind a "Click here to see the privacy settings" button. In the latter case, that opened for information avoidance, and a larger share logged in with their Facebook account, thereby giving up their privacy, than in the group that were given the privacy information by default.

The growing literature on the economics of privacy and privacy behavior is mainly interested in the trade-off between keeping personal information private or sharing it with others, often commercial actors (Acquisti et al., 2016). Individuals share their personal information to gain a benefit, such as a better service, a personalized and more relevant advertisement, or a discount. Personal data contain information that can be of value not only to commercial actors, but also to policymakers and law makers (Acquisti et al., 2013). In addition, the use of data could also benefit the individual, but, as both consumers and citizens, the individuals must bear the privacy risk of, for example, potential data abuse (Acquisti et al., 2015). The *privacy calculus theory* describes how consumers must be able to weigh the benefits of using a digital service that entails sharing data against the risk of reduced privacy (Dinev and Hart, 2006; Fox et al., 2021; Keith et al., 2013). To make this choice or calculation, one would expect the individual to seek a lot of information, as long as transaction costs are low, and this information-gathering process is the

focus of our study. How individuals handle this trade-off has led to literature on what is known as the *privacy paradox*, according to which there is a lack of consistency between how people state that they value their digital privacy and their intentions to protect the data, and what they actually do to protect them (Norberg et al., 2007). In a review article, Kokolakis (2017) finds that there is no consensus in the literature regarding this paradox. However, it is widely acknowledged that the handling of privacy in the digital sphere, understanding and controlling how personal data are harvested, stored, used, and shared when using a large variety of online services regularly, is a complex and difficult task (Acquisti et al., 2020, 2007, 2016; Athey et al., 2017; Gómez-Barroso, 2018; Solove, 2012).

Behavioral economics studies focus on consumers' behavioral biases and heuristics, which play an important role in privacy decisions (Acquisti et al., 2020, 2007), and can contribute to a better understanding of choices that are not in line with the classical economic theory of information. For example, John et al. (2011) show how varying the layout of a website, even when the variations have no connection to privacy and everything else is kept equal, makes participants in different experiments behave differently in terms of sharing very personal data. Other privacy studies focus on how consumers' choices can be related to personal characteristics, such as how concerned or knowledgeable they are about privacy, whether they suffer from privacy fatigue, and whether they trust the company concerned or not (Alfnes and Wasenden, 2022; Choi et al., 2018). In our study, we measure common variables in studies of privacy choice, such as privacy concerns and trust in the actor collecting data.

Privacy decisions often consist of multiple consecutive stages and various decisions, not just one single decision. For example, when using social media, you first decide your privacy settings, with whom you share what, and then decide what to actually post on your wall or profile page. Similarly, when performing an online search, you first decide on the search engine and, after that, you conduct the actual search. Adjerid et al. (2019) study how the choice architecture of such sequential choices could affect final outcomes. Most research has been done on the downstream level, what is actually shared, and less on the upstream settings. The choice between seeking out or avoiding privacy information would add a new layer to their model.

As described above, the decisions individuals have to take regarding the sharing of personal data are not easy. The complexity of weighing the potential privacy risk of sharing too much against the loss of a benefit, for example by receiving less valuable services, is high. In

such situations, turning back to classical economic theory, and searching for as much information as possible sounds like the reasonable thing to do. However, casual evidence tells us that decisions are quite often made without the decision-maker seeking available information. A variety of factors would have an impact on whether or not individuals seek out or ignore information when making privacy decisions. On the one hand, someone who is concerned about privacy would be interested in the information in order to reduce the risk, while, on the other hand, someone suffering from privacy fatigue could be in a state where she just says yes. If the decision-makers trust the data collector, they are more likely to say yes to sharing without seeking information. The time cost, how much time it would take, and the risk that the information will be so complex that the readers will not be able to understand it even if they spend a significant amount of time on it, might cause more information avoidance. Returning to the model of Sharot and Sunstein (2020), hedonic well-being could play a role in information avoidance. If something in the privacy information could be perceived as unpleasant, the individual might want to avoid it. There is a well-established link in the literature between entertaining media content and hedonic well-being (Rieger et al., 2014). In this study, we contribute to a better understanding of the potential link from the level of hedonic well-being induced by the level of entertainment of the content consumed, via elements of the privacy information that could reduce this well-being, and ultimately to information avoidance.

### **3 Hypotheses and measurements**

The main element of the experiment is a variation in the content of the videos that the participants watched. In addition, we also introduce a treatment variation in the time cost of gathering privacy information. The first treatment provides insight that is relevant to our main research question *“Are people less likely to seek out privacy information when consuming more entertaining content compared to less entertaining content?”* Similarly, the second treatment provides insight that is relevant to the secondary question: *“Does the time cost of obtaining information affect the likelihood of seeking the privacy information?”* We also study the interaction effect between the content of the video and a higher time cost of reading.

We base our main hypothesis on the logic from the model by Sharot and Sunstein (2020). The consumption of entertaining media content will contribute to hedonic well-being. The pri-



privacy information could potentially have a negative impact on the experience of consuming the entertaining content in the same way as nutrition information could ruin a tasty but not-so-healthy meal. We also tested the logic in a pre-experiment survey (more details in appendix A) where respondents were randomized into two groups, one focusing on an online situation where they were shown entertaining content, and one group assigned to an online situation without further specification. A larger share of the first group reported that they believed privacy information could ruin or negatively impact their experience. We formulate the following hypothesis:

**Hypothesis 1.** *Participants consuming more entertaining content are less likely to access privacy information than participants consuming less entertaining content.*

Turning to *time cost* and the fact that time is a transaction cost (DeSerpa, 1971), we expect a longer indicated reading time to reduce the likelihood of accessing privacy information, and we formulate the following hypothesis:

**Hypothesis 2.** *Participants who are given an indication of a longer reading time are less likely to access privacy information than participants who are given an indication of a shorter reading time.*

To provide further insight into the link from entertaining content, via hedonic well-being to information avoidance, based on Sharot and Sunstein (2020) and the pre-experiment survey, we asked participants in our experiment about their expectations about how accessing the privacy information would influence their user experience. We measured this through a question in the exit survey. We formulated our last hypothesis as follows:

**Hypothesis 3.** *Participants who expect that reading the privacy notice will negatively affect their user experience are more likely to avoid privacy information than participants who expect a less negative effect.*

The key measurement in our study is whether or not the participants actually access the

privacy information and decide to open the privacy notice.<sup>1</sup> Two important additional measures are secondary beliefs about entertainment and the time that the participants spend. The first is an incentivized question about how large a share of participants the individual in question believes found the first video entertaining. This gives us a measure at the individual level of entertainment, as it will be the personal experience of watching the video that forms the basis for beliefs about how entertained other participants were. Our time measure is the time spent on every step throughout the experiment, including the time they spend making their decision on whether or not to open the privacy notice. As these are secondary outcome variables, we do not formulate hypotheses about the effects, but we will look at differences in the time the participants take to decide in relation to our research questions and hypotheses to examine whether the treatments have an effect on time spent. We also use this second outcome measure to compare *information gatherers* and *information avoiders* across treatment groups, and we can compare fast and slow decision-makers. Finally, in the exit survey, we measure relevant covariates such as risk profile, trust in the service provider, privacy concern, and how much they enjoyed the videos. These were all measured using 5-point Likert scales. See Appendix B for details.

## 4 Experimental Design

The main set-up for the experiment consisted of participants watching and rating two videos. Between the two videos, they had to make a decision about whether or not to access privacy information.<sup>2</sup> The participants were randomly assigned to two groups watching videos with high or low levels of entertainment. In addition, we randomly split the participants into two further subgroups, varying the indicated time cost of seeking privacy information. The participants were recruited through the crowd-sourcing platform Prolific Academic and the experiment was conducted in May 2022. The main features of the 2x2 design are illustrated in figure 1.

### 4.1 Introducing the task, consent form and privacy saliency

The participants read through a consent form and an information page before watching the first video. We informed the participants that they were being asked to watch videos and rate them.

---

<sup>1</sup>Due to the variation in time cost, the participants who decide to open the notice are forced to wait for 10 or 30 seconds. For this reason, combined with the fact that they actually open the notice, we find it likely that they actually read the content

<sup>2</sup>Screenshots from the experiment are provided in appendix B

In the consent form, we gave them accurate information about privacy, and how we handle data. In our case, the data are handled in compliance with European Privacy Regulations, GDPR (General Data Protection Regulation). In addition to the information about the handling of personal data, participants were informed that they could leave at any time during the experiment.

When the participants had accepted the general terms for the task, they were asked to answer two questions about the information they had just received, as comprehension checks. If their answers were wrong, they were redirected to read the consent and information forms again. They were given an opportunity to answer the attention check questions a second time. One of the questions in the attention check is about the privacy terms of the study, which helps to make the participants aware of privacy. If they gave wrong answers for a second time, they were not allowed to continue the study. We also asked if the participants knew of the company Telenor before starting the study, to control for the effects of the potential familiarity with the brand.

#### 4.2 Videos - content treatment

For the study, we used four different videos produced by Telenor. Two of them are entertaining commercials, both related to how mobile technology could be useful. The two other videos are informative and made for brand-building purposes; one focuses on cyber-bullying, while the other explains how mobility data from the mobile network could be used to understand the spread of diseases. To select the videos used in our study, we ran a pre-test of the videos, also using the





	Content	
Time cost	Entertainment	Informative
10 Secs	 + short time	 + short time
30 Secs	 + long time	 + long time

Figure 1: Experimental design: We use a 2x2 design in which we manipulate the content and the time cost of reading the privacy notice.

Prolific platform.<sup>3</sup> In the pre-test, we included six videos, three that could be considered more entertaining and three that had a more informative and educational content. Participants in the pre-test watched all the videos and were asked to rate their level of entertainment on a 5-point Likert scale. In the experiment, we used the videos that scored highest and lowest on entertainment. The participants in the *Informative* treatment watched two videos with a low entertainment level the one with the lowest level first (*Informative video 1* followed by *Informative video 2*). Those in the *Entertain* treatment watched two videos with high entertainment levels, the one with the highest level first (*Entertaining video 1* followed by *Entertaining video 2*). All four videos used in the experiment were available online at the time of writing.<sup>4</sup>

### 4.3 Privacy notice and time treatment

At the beginning of the first video, there is a quick reminder about the privacy terms, and the only choice given to participants is to continue to the video. The pop-up shows the following text: “*Privacy Reminder. For this video, your personal data will be handled as described in the consent form.*”. At the beginning of the second video, there is another message about privacy. In this case, the pop-up warns about a potential change in the privacy policy. The message is as follows (either 10 or 30 seconds is shown): “*The privacy policy might be different for this video. You can read about the privacy policy for this video by clicking the ‘Read the policy’ button. Reading the policy may take at least 10 (30) seconds. You can also go directly to the video by clicking on the ‘Agree to the policy’ button.*”. The participants have to choose whether they want to read the privacy information or avoid it and proceed directly to watching the video by agreeing to the policy without reading it. Since the participants are informed on the consent page that they can leave the study at any point if they do not want to choose either of the two options, they are allowed to leave the study. If they decide to leave, they will not be paid for their participation. A randomized half of the participants are told that reading the notice will take at least 10 seconds, while the other half are told that it will take at least 30 seconds. Figure 2 shows the flow of the experiment with the two treatments. The actual content of the privacy notice is the same as on the consent page, with no actual changes to the privacy policy. The participants who chose to

---

<sup>3</sup>For more information about the pre-test, see Appendix A

<sup>4</sup>Informative video 1: <https://www.youtube.com/watch?v=1xMZjt84CNg>, Informative video 2: <https://www.youtube.com/watch?v=z0MLbKoU28w>, Entertaining video 1: <https://vimeo.com/13555757>, Entertaining video 2: <https://www.youtube.com/watch?v=GDLU5Y8fmzk>. All videos viewed December 28, 2022.

read it were kept waiting for 10 or 30 seconds, depending on the time treatment, before they were allowed to move on to the second video.

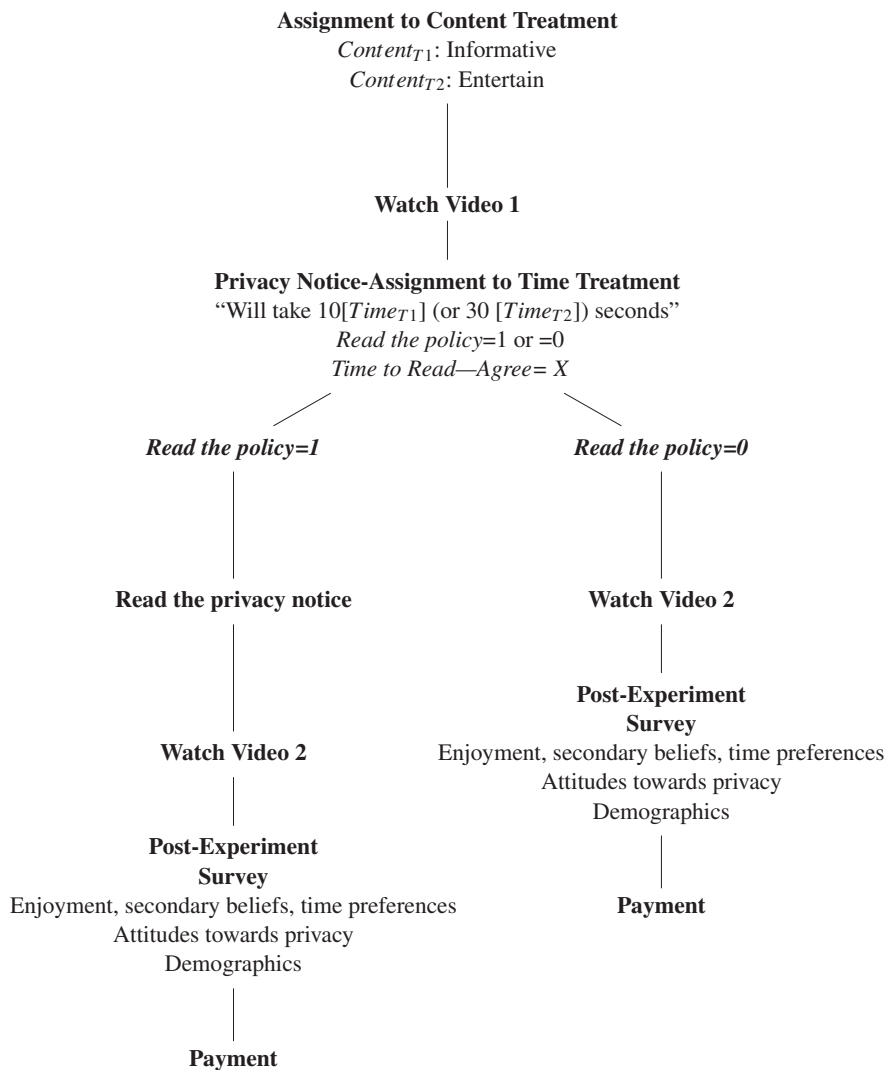


Figure 2: Experimental Design

**Note:** In both the *Informative* and *Entertain* treatments, participants first watch Video 1. After finishing the video, before watching Video 2, they are shown a pop-up informing them that the privacy policy may be different for this video. They are asked to choose whether to read the policy or agree and continue watching the video. In this pop-up, they are informed that reading the privacy information will take at least 10 seconds in the  $Time_{T1}$  and 30 seconds in the  $Time_{T2}$ . If they choose to read it, they will not be able to watch the video for the stated time period. If they choose not to read it, they can watch Video 2 directly. After watching both videos, behavioral measures, attitudes and demographics that are listed as control variables will be collected in the post-experiment survey.

## 4.4 Post-experiment survey

In the post-experiment survey, the participants were asked how much they enjoyed the two videos they watched, followed by two simple questions about the main characters/topics of the videos as attention checks. If they failed the test, they were given a second chance to answer, and if they failed twice, they were not allowed to continue the experiment. They were then asked about their expectations of what reading the privacy information could do to their user experience and their secondary beliefs about the level of enjoyment the first video gave to the other participants in the study (this question was incentivized with a bonus payment). We also measured additional covariates, such as basic demographics, risk preferences, and privacy concern. Lastly, time preferences were elicited through a time discounting task. In addition to the information that we collected, we received more demographic information about country of residence and birth, and employment status from Prolific’s database.

## 5 Sample and procedures

Following a pre-experiment survey and a pre-test of the videos, the sample size estimation, hypotheses and the main design of the present experiment were pre-registered via the American Economic Association’s RCT Registry (Ay et al., 2022).<sup>5</sup> We targeted participants outside the company’s commercial footprint to avoid them being biased due to prior knowledge of the company.

### 5.1 Sampling procedures

We recruited our participants from the crowd-sourcing platform Prolific Academic in May 2022, with a target of around 400 subjects in each of the four sub-samples. We ran each treatment separately on different weekdays, Mondays to Thursdays, starting at the same time of day.<sup>6</sup> Each participant could only participate in one treatment, including the pre-test of the videos. The whole experiment took seven minutes on average and the average earnings were about 3\$. The participants were permanent residents of the USA or Canada, aged 18 to 70 and fluent in English. The participants had to have a minimum acceptance rate at Prolific of 97 percent, and had to

---

<sup>5</sup>For details about the pre-tests see Appendix A

<sup>6</sup>This is a common way of ensuring randomization at Prolific, as discussed here: <https://community.prolific.co/t/random-assignment-to-different-survey-versions/4834>

have completed a minimum of 200 studies. Finally, we filtered to obtain an equal gender balance among participants. In addition to these selection filters, we carried out a comprehension check after introducing the task and two attention checks during the task, in order to ensure the quality of the answers. The drop-out rate was around 35 percent.

## 5.2 Sample preparation and matching

Due to unforeseen external events, we had problems with Prolific during the data collection. When collecting the “Entertainment 30” treatment, the last of the four sub-samples, the answers came in more slowly than they had for the other sub-samples, following a different pattern. After checking activities on the Prolific page at reddit we found that a major US company had launched a big task that strongly reduced the capacity of the platform.<sup>7</sup> We ended up with a sample that did not balance well, and decided to re-run the sub-sample at a later date. This time, the activities started normally, but answers stopped coming in after a while. It turned out that this happened when the Uvalde school shooting became known in the media.<sup>8</sup> We paused the experiment, but restarted it the next day and left it open longer than we had initially planned for. After the different rounds, we had 953 participants with valid answers instead of our target of around 400 in the “Entertainment 30” treatment. To keep the treatment effects isolated from potential differences in sample characteristics, we used propensity score matching to pick subjects based on gender, age, and country of residence. By using so-called nearest neighbour greedy matching, we aimed to adjust the bias based on observable characteristics between the treatment groups (Hirano et al., 2003; Rosenbaum and Rubin, 1983). We matched the participants in the “Informative 30” treatment with the “Entertainment 30” participants with the least distance between observable characteristics. Descriptives of the final samples can be seen in Table 1.

---

<sup>7</sup><https://www.reddit.com/r/ProlificAc/>

<sup>8</sup>[https://en.wikipedia.org/wiki/Robb\\_Elementary\\_School\\_shooting](https://en.wikipedia.org/wiki/Robb_Elementary_School_shooting)



Table 1: Summary descriptives table by ‘treatment’ groups

	Ent.10	Ent.30	Nor.10	Nor.30
	N=398	N=400	N=398	N=402
Age	37.7 (12.6)	37.4 (12.8)	38.0 (12.5)	38.2 (13.5)
Gender:				
Female	49.2%	49.8%	49.7%	48.8%
Country of Residence:				
United States	83.2%	89.7%	75.6%	90.5%
Number of Rejections in Prolific	3.08 (3.44)	2.91 (3.15)	3.06 (3.98)	3.31 (3.62)
Familiarity with Telenor:				
No	97.2%	99.3%	97.2%	98.3%

*Note:* Participants are well randomized into treatments across demographics reported in the table with  $p > 0.1$ , except for the Country of Residence. In Nor. 10, the share of participants from Canada is higher compared to other treatments.

## 6 Results

In the following we will report the results of our treatments and relevant covariates on the share of readers. In addition, we will look for patterns related to the treatments and at the time participants spent making their decision. We will also look at differences in the expected effect of reading the privacy information and take a closer look at the information avoiders.

### 6.1 Share of information avoiders

Figure 3 shows the share of participants in the four sub-samples that decided to seek information and read the the privacy form. This share ranges from 22 percent in the group with informative content and a short indicated reading time, to 17 percent in both the sub-samples with a long indicated reading time. The share of information seekers in the group watching entertaining videos with a short reading time is 19 percent. These numbers show a tendency towards a decrease in the share that reads the information, especially as regards the time cost, but also for

entertaining content. In Table 2 we report results from a logistic regression with a dummy taking the value one if the participant read the privacy information and zero if not, as dependent variable. First, turning to our two main treatments, results indicate that the content treatment does not have a significant effect, while the time treatment has an effect in line with our second hypothesis. In column one, we report the results of the two treatments, including non-significant control variables, as described in the note to the table. In the second column, the interaction between the two treatments is also non-significant.

In the third column, we include relevant covariates, measured in the exit survey after the experiment. The respondents' risk preferences, privacy concern, trust in Telenor, and time preferences are included. They are all measured using a 5-point Likert scale, and we have constructed dummy variables where those answering the two highest levels are given the value one. Trust can serve as an example. Those saying they "agree" or "strongly agree" with a statement that they consider Telenor trustworthy are given the value 1. We see from the third column in Table 2 that a high level of trust in Telenor is negatively correlated with reading the privacy information, that fewer participants read the privacy information if they have high trust, while high levels of privacy concern make it more likely that the information will be read. This is what we would expect based on findings in other privacy studies (e.g. Alfnes and Wasenden (2022)). We also find a lower reading probability among risk takers.

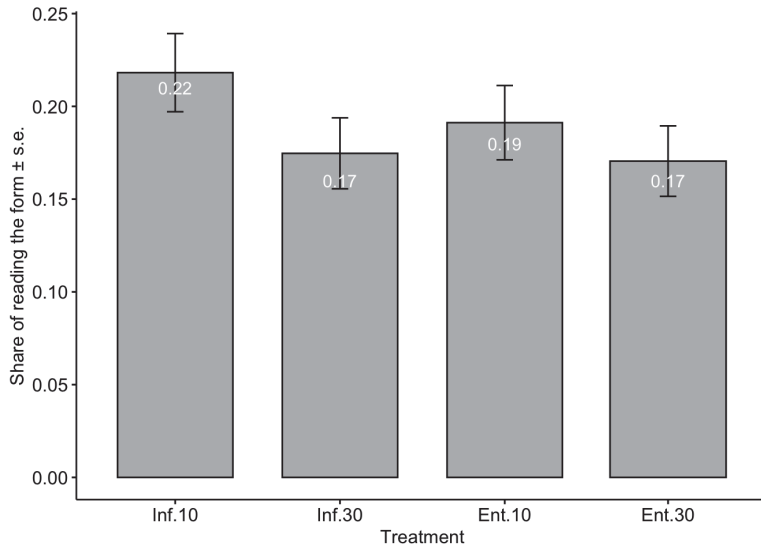


Figure 3: Share of readers in all treatments

We also measure the level of entertainment through secondary beliefs about the level of entertainment among other participants. In Table 3, we report results using this alternative measurement of entertainment levels, which shows a slightly different picture. The first regression, only including the measures for entertainment and time cost, and controls, shows significant reductions in both dimensions, which is in line with our two first hypotheses. However, when including the interaction, only the entertainment measure yields a significant result. Finally, when the covariates are included, we do not find significant results, neither for the secondary beliefs about entertainment, the time treatment nor the interaction between them, even though the point estimates are all negative, as we would expect.

In our first two hypotheses, we predicted that fewer participants would seek out privacy information among those who were watching more entertaining content and among those exposed to a long indicated reading time. Our findings give indications that these hypotheses might be correct, but our results are somewhat inconsistent, and invite further research to gain a better understanding of these relationships.

Table 2: Logistic regression - reading privacy information - content and time treatment

Dep. var.:			
Reading the privacy information	(1)	(2)	(3)
Entertain	-0.141 (0.129)	-0.197 (0.177)	-0.169 (0.179)
30 seconds	-0.242* (0.130)	-0.300* (0.181)	-0.323* (0.181)
Entertain × 30 seconds		0.121 (0.259)	0.156 (0.261)
Risk taker			-0.153** (0.064)
Privacy concerned			0.309* (0.161)
High trust			-0.384*** (0.134)
Present biased			-0.191 (0.138)
Constant	-1.612*** (0.274)	-1.589*** (0.278)	-1.135*** (0.370)
Demographic controls	YES	YES	YES
Observations	1596	1596	1596

*Notes:* The table reports logit coefficients of regressing the content and time treatments on the *Read the privacy information dummy* for the full sample. The treatments are measured through dummies, and the entertainment dummy is one if the participant watched a highly entertaining video, and otherwise zero, while the time dummy is one if the participants were given an indication of a long reading time (30 seconds) and zero for a short reading time (10 seconds). The treatments “High entertainment level” and “High indicated reading time” are compared to low levels of the same. In column (2), we add the interaction between the treatments, while, in column (3), we add additional covariates: self reported risk taker, high level of privacy concern, high trust in Telenor(the company in the experiment), and present bias. We also include a set of demographic controls in the regression that are not significant, without reporting the details: age, gender, prior knowledge of Telenor, and US resident. Standard errors are in parentheses. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

Table 3: Logistic regression - reading privacy information - secondary beliefs about entertainment levels and time treatment

Dep. var.:			
Reading the privacy information	(1)	(2)	(3)
Secondary beliefs about entertainment	-0.779*** (0.267)	-0.678* (0.366)	-0.418 (0.374)
30 Seconds	-0.252* (0.130)	-0.110 (0.370)	-0.083 (0.373)
Secondary x 30 seconds		-0.216 (0.526)	-0.258 (0.531)
Risk taker			-0.143** (0.064)
Privacy concerned			0.304* (0.160)
High trust			-0.331** (0.136)
Present biased			-0.196 (0.138)
Constant	-1.239*** (0.306)	-1.308*** (0.356)	-1.031** (0.420)
Observations	1596	1596	1596

*Notes:* The table reports logit coefficients of regressing the secondary beliefs about entertainment and time treatments on the *Read the privacy information dummy* for the full sample. The secondary beliefs are a continuous normalized variable running from 0.01 to 1, and the time dummy is one if the participants were given an indication of a long reading time (30 seconds) and zero for a short reading time (10 seconds). The treatment “High indicated reading time” is compared to low reading times. In column (2), we add the interaction between the treatments, while in column (3), we add additional covariates: self reported risk taker, high level of privacy concern, high trust in Telenor (the company in the experiment), and present bias. We also include a set of demographic controls in the regression that are not significant, without reporting the details: age, gender, prior knowledge of Telenor, and US resident. Standard errors are in parentheses. \*\*\* - significant at 1 percent, \*\* - significant at 5 percent, \* - significant at 10 percent.

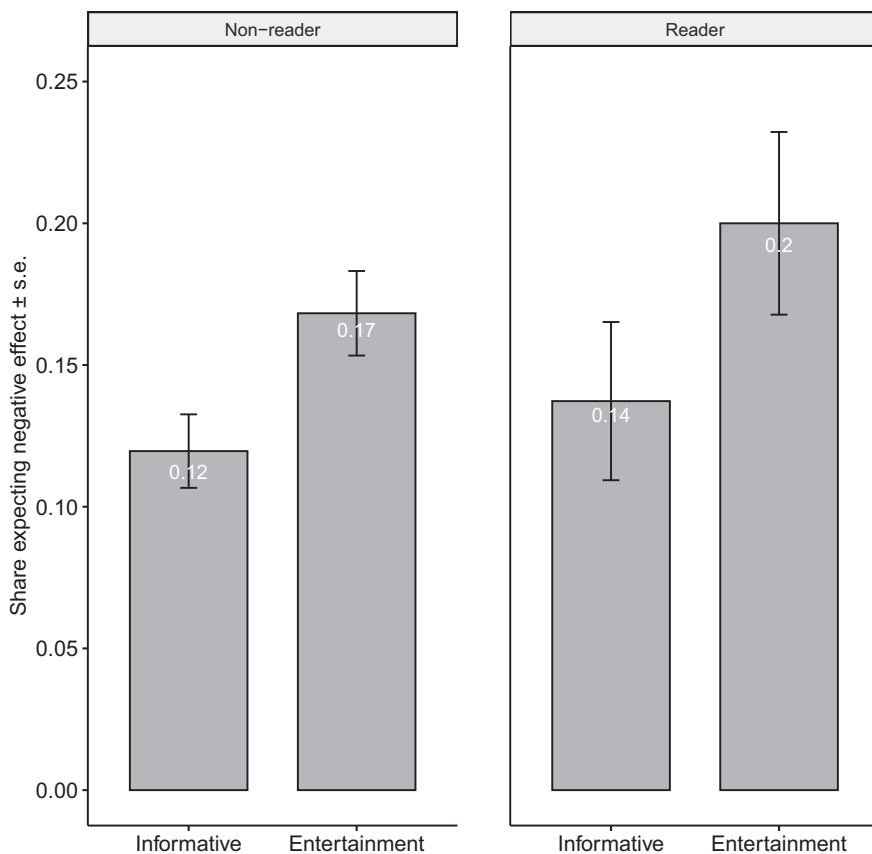


Figure 4: Share of those who expect a negative effect in treatments grouped by readers and non-readers.

## 6.2 Expectations of the effects of reading the privacy information

As part of the exit survey, we asked the participants how they believed reading the privacy information would affect their experience of watching the second video, using a Likert scale ranging from very positive to very negative. For this question, there is a difference between those who read it and know the content of the privacy information, and those who did not read it and were still ignorant. The readers and non-readers are not directly comparable. For that reason, our experiment is not well suited to testing hypothesis 3.

However, by splitting the sample into readers and non-readers and studying these groups

individually, we can compare participants who have the same information and are similar. When looking at the shares that expect a negative experience for each content treatment in these sub-groups, we see an interesting pattern. As shown in Figure 4, the share of the non-readers who are exposed to highly entertaining content who expected a negative experience is significantly higher than in the group exposed to less entertaining videos, at 17 and 12 percent, respectively. We see a similar pattern, although not significant, in the sub-roup of participants who actually read the privacy information.

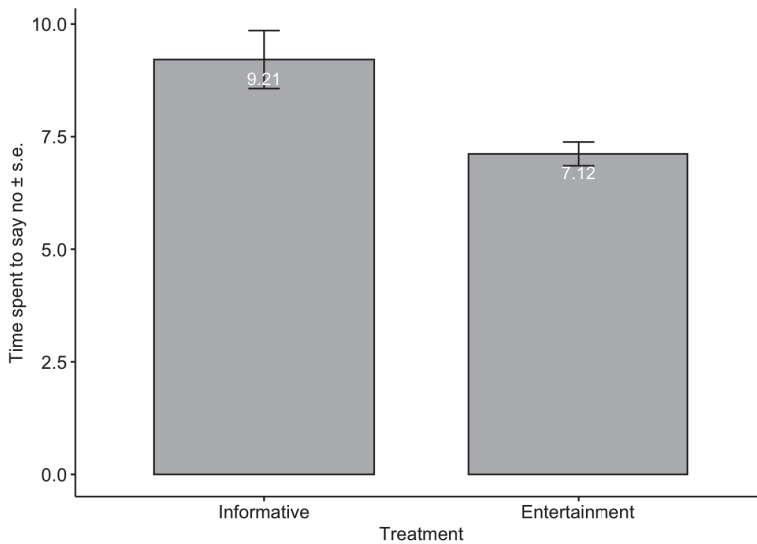


Figure 5: Time spent on deciding whether or not to read the privacy notice

### 6.3 Fast and slow decisions and decision-makers

How quickly the participants take their decision to read or not read might give us insights into the decision-making process, and we also carry out exploratory analysis that are based on decision time. As we saw in Figure 3, almost 80 percent of the participants chose not to access the privacy information and read the notice before watching the second video. Figure 5 shows how much time these non-readers spent on deciding not to read the notice, split between the entertaining and informative content groups. The informative group took on average 9.2 seconds to make their decision, while the group watching entertaining content made their decision significantly more quickly, with an average of 7.1 seconds. Turning to those who decided to read, on average,

the informative group spent 12.5 seconds and the entertainment group 10.8. This difference is not significant. We also note that non-readers spent less time making their decision than readers. This finding gives us a hint that content does play a role in decisions about whether or not to seek privacy information.

## 7 Conclusion

Through this study, we provide new evidence on how privacy decisions, and more specifically decisions to avoid or seek privacy information when consuming online media content, are made. Firstly, we find that, even within a closed environment specifically set up for research, around 20 percent of the participants, regardless of the content and the time cost, decide to read the privacy information. It is not surprising that participants find it unlikely that their personal data will be misused when performing a task for a research project at Prolific, leading to lower shares of readers. Even though a fairly high share decided to seek the information, around 80 percent do not read it and avoid the information. For policy-makers it should be kept in mind that asking service providers to make information available does not mean that individuals actually access the information and learn from it.

Then, returning to our main topic, inspired by Sharot and Sunstein (2020), who find that entertaining content makes people avoid privacy information, we find clear indications that our treatment has effects that support our hypothesis. All our point estimates indicate a lower reading probability among those exposed to entertaining content. We also find some significant results. In addition, we find other indications that differences in content have an effect on such privacy decisions. First, our results show that those who are exposed to entertaining content make their privacy decisions more quickly than those exposed to informative content. Furthermore, we observe a significantly higher share of participants in the entertaining group who expect a negative effect on their experience, among those who decided not to read. We do not ask specifically what kind of negative information they expect to receive, but one possibility is that it could be of the same type and have the same effect as nutritional information has on the enjoyment of a tasty but not-so-healthy meal (Sunstein, 2019).

Our results indicate a direction of the effects of the content and the time cost even though it is not strongly significant, and we believe that more research should be conducted to study how



differences in content can trigger different privacy decisions. Privacy behavior and information avoidance could be further investigated and mapped in relation to the various types of content consumed in everyday digital life. Reisch et al. (2021) conclude that policy-makers should also consider the hedonic effects of information in the food policy context. More research on this potential effect should also be carried out for privacy. If, under certain circumstances, learning about privacy could reduce peoples well-being, this could imply that policy should have a wider scope in this area as well.

Finally, the decision whether to seek out or avoid information must be seen in relation to other inter-related privacy decisions. Adjerid et al. (2019) argue that privacy choices are quite often made in different steps. For example, when using social media, you first decide on your privacy settings, with whom you share what, and then decide on what to actually post on your wall or profile page. They argue that most research has been done on the downstream level, what is actually shared, and less on the upstream settings. To better understand the privacy decision process, research on choice architecture should also include the information-seeking layer.

## References

- Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509–514.
- Acquisti, A., Brandimarte, L., and Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4):736–758.
- Acquisti, A., Gritzalis, S., Lambrinouidakis, C., and di Vimercati, S. (2007). What can behavioral economics teach us about privacy? In *Digital privacy*, pages 385–400. Auerbach Publications.
- Acquisti, A., John, L. K., and Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, 42(2):249–274.
- Acquisti, A., Taylor, C., and Wagman, L. (2016). The economics of privacy. *Journal of economic Literature*, 54(2):442–92.
- Adjerid, I., Acquisti, A., and Loewenstein, G. (2019). Choice architecture, framing, and cascaded privacy choices. *Management Science*, 65(5):2267–2290.
- Alfnes, F. and Wasenden, O. C. (2022). Your privacy for a discount? exploring the willingness to share personal data for personalized offers. *Telecommunications Policy*, 46(7):102308.
- Athey, S., Catalini, C., and Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. Technical report, National Bureau of Economic Research.
- Ay, F. C., Freddi, E., and Wasenden, O. C. (2022). Strategic ignorance and privacy - would entertaining content trigger information avoidance? *AEA RCT Registry*, AEARCTR-0009406.
- Bergemann, D., Bonatti, A., and Gan, T. (2022). The economics of social data. *The RAND Journal of Economics*.
- Choi, H., Park, J., and Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81:42–51.
- DeSerpa, A. C. (1971). A theory of the economics of time. *The economic journal*, 81(324):828–846.

- Dinev, T. and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, 17(1):61–80.
- Fox, G., Clohessy, T., van der Werff, L., Rosati, P., and Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, 121:106806.
- Golman, R., Hagmann, D., and Loewenstein, G. (2017). Information avoidance. *Journal of economic literature*, 55(1):96–135.
- Gómez-Barroso, J. L. (2018). Experiments on personal information disclosure: Past and future avenues. *Telematics and Informatics*, 35(5):1473–1490.
- Hirano, K., Imbens, G. W., and Ridder, G. (2003). Efficient estimation of average treatment effects using the estimated propensity score. *Econometrica*, 71(4):1161–1189.
- Hoofnagle, C. J. and Whittington, J. (2013). Free: accounting for the costs of the internet's most popular price. *UCLA L. Rev.*, 61:606.
- John, L. K., Acquisti, A., and Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, 37(5):858–873.
- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies*, 71(12):1163–1173.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64:122–134.
- Loewenstein, G. and O'Donoghue, T. (2006). "we can do this the easy way or the hard way": Negative emotions, self-regulation, and the law. *The University of Chicago Law Review*, 73(1):183–206.
- Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1):100–126.
- Reisch, L. A., Sunstein, C. R., and Kaiser, M. (2021). What do people want to know? information avoidance and food policy implications. *Food policy*, 102:102076.

- Rieger, D., Reinecke, L., Frischlich, L., and Bente, G. (2014). Media entertainment and well-being—linking hedonic and eudaimonic entertainment experience to media-induced recovery and vitality. *Journal of Communication*, 64(3):456–478.
- Rosenbaum, P. R. and Rubin, D. B. (1983). The central role of the propensity score in observational studies for causal effects. *Biometrika*, 70(1):41–55.
- Sharot, T. and Sunstein, C. R. (2020). How people decide what they want to know. *Nature Human Behaviour*, pages 1–6.
- Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, 126:1880.
- Stigler, G. J. (1961). The economics of information. *Journal of Political Economy*, 69(3):213–225.
- Sunstein, C. R. (2019). Ruining popcorn? the welfare effects of information. *Journal of Risk and Uncertainty*, 58(2):121–142.
- Svirsky, D. (2022). Privacy and information avoidance: An experiment on data-sharing preferences. *The Journal of Legal Studies*, 51(1):63–92.
- Sweeny, K., Melnyk, D., Miller, W., and Shepperd, J. A. (2010). Information avoidance: Who, what, when, and why. *Review of general psychology*, 14(4):340–353.
- Utz, C., Degeling, M., Fahl, S., Schaub, F., and Holz, T. (2019). (Un) informed consent: Studying gdpr consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security*, pages 973–990.

## A Pre-experiment Survey and Pre-test of the Videos

Prior to running the main experiment, we ran a pilot with a survey experiment to see how general privacy preferences are shaped when the content changes among representative samples of 1000 respondents from the US and Norway. In the survey, we wanted to test our main idea, that the level of entertainment of online content has an impact on what people expected to experience as a result of receiving privacy information. We randomized the respondents to one group considering a situation in which they used a service they “regularly use to be entertained” and the other group to a service they “regularly use”. We then asked them to consider a situation in which they receive accurate information about how their personal data will be used by the service provider, and how likely it is that this would negatively impact the experience of using the service. As reported in Figure 6, we found that in the USA a significantly higher share reported that they believed that privacy information would have a negative impact on their experience.

Following the pre-experiment survey, we ran a pre-test with 6 videos in total to select which ones to use in the main experiment. A hundred participants were recruited in Prolific Academic for the pre-test. In Figure 6, we report the levels of entertainment, measured on a 5-point Likert scale, for the 6 videos tested. We selected the videos for the main experiment based on this pre test, using *Young Love* and *The Essay* as highly entertaining videos and *Dengue Fever* and *Online Safety* as informative videos.

How likely is it that the actual information would negatively impact your experience?  
US vs. Norway

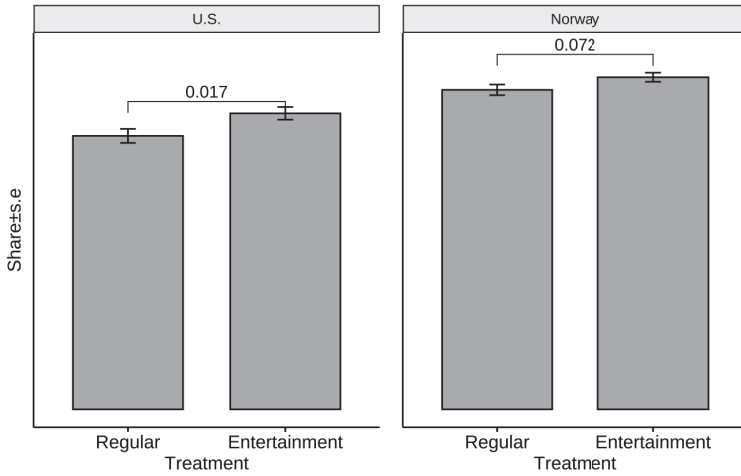


Figure 6: Main content treatment in the pilot experiment

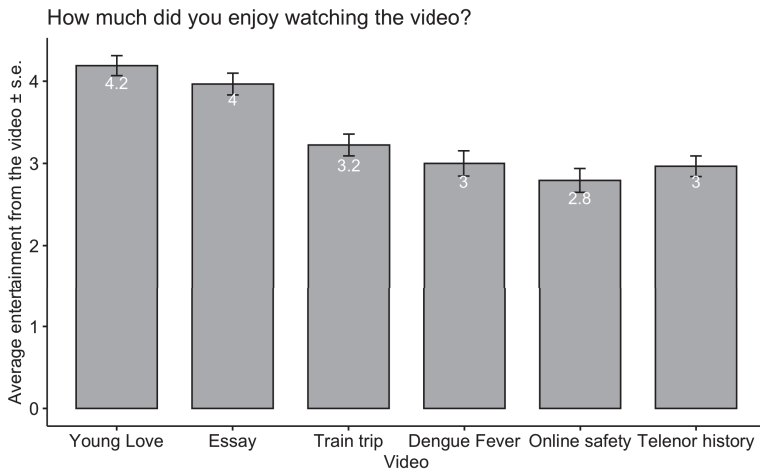


Figure 7: Entertainment levels of videos in the pre-test

## **B Screenshots from the experiment**

In the following, screenshots from all elements of the experiment are added.

---

## Welcome

Welcome to this study run by Telenor Research, the research branch of the multinational telecommunication operator Telenor. For more information about Telenor you can click [here](#). If you agree to take part, the entire study will last about 8 minutes.

### Procedures

You will be shown two different videos and will be asked to answer questions about these videos after watching them. This study does not involve deception and it has been approved by an internal review board.

### Participation

Participation in this study is voluntary. You have the right to withdraw at any time or refuse to participate entirely, without jeopardy to future participation in other studies conducted by us. You can discontinue the study at any time, but you must complete all parts to be eligible to receive your payment.

### Privacy policy

Your answers and actions during this task will be recorded and will be used by Telenor in compliance with European Privacy Regulations—GDPR (General Data Protection Regulation). The collected data can be used for research, brand management and marketing. All collected data will be kept confidential, and no one other than the responsible researchers will have access to them. The data will be anonymized, only reported in an aggregate format, and identifying individuals will not be possible. A secure server, which can only be accessed by the responsible researchers, will be used for storage and analysis of the data.

### Payment

Your payment for participating in this study will consist of a participation fee of 1 GBP and a potential bonus payment of 0.1 GBP. The participation fee will be sent to you after the completion of this survey. You can also earn a bonus payment based on your answers to some of the questions. You will receive the bonus when the data collection is completed.

### Completion

You will receive a completion link at the end of the study.

### Questions about the study

If you have questions regarding this study, you may contact: [ole-christian.wasenden@telenorresearch.com](mailto:ole-christian.wasenden@telenorresearch.com)

**If you agree to take part in the study, please check the box below.**

I certify that I am 18 years or older. I have read this consent form and I agree to take part in this study.



## Thank you for participating in our study

In this task you are asked to watch and rate two videos by Telenor.

**Please watch the videos carefully**, as you will be asked some questions about their content, your rating of the videos, as well as your feelings while watching them. Your honest opinion will be very valuable for us.

If your answers indicate that you have not watched the videos, you will not be able to complete the task.

You will be shown the two videos one after the other before proceeding to the set of questions. The videos will automatically start and proceed, and you will not have the chance to pause and replay them. Therefore, before proceeding to the next page, please make sure you will **be able to watch the videos for a duration of 3.5 minutes without interruptions**.

For technical reasons, the allocated time for completing the first part of the study is fixed regardless of your choices, therefore you may have to wait if you are done with your actions before the timing is over.

### Important information about this task:

- Do not refresh pages or open multiple tabs with the task URL.
- We ask you to use Chrome or Edge and to activate your pop-ups for this URL since you may receive messages through them.
- You will not be able to navigate back once you have proceeded to a next page.

Next

## We want to make sure you comprehend the terms of this study

It is important for your participation in this study that you read the information provided in the previous pages.

**Please answer the two questions below**, so we can make sure that you understand and consent to the terms of the study.

**If you submit incorrect answers you will be automatically redirected to the consent form. And if you submit incorrect answers the second time, you will not be able to continue.**

### Question 1

You personal data that are collected in this study will be handled according to ...

- The data protection act    The consumer privacy act    European Privacy Regulations  
 The Gramm-Leach-Bliley act

### Question 2

During the study, you will be able to ...

- Pause and replay the videos    Leave at any point you want    Mute the videos  
 Refresh the browser anytime

Next

## We want to make sure you comprehend the terms of this study

It is important for your participation in this study that you read the information provided in the previous pages.

**Please answer the two questions below**, so we can make sure that you understand and consent to the terms of the study.

**If you submit incorrect answers you will be automatically redirected to the consent form. And if you submit incorrect answers the second time, you will not be able to continue.**

### Question 1

Your personal data that are collected in this study will be handled according to ...

- The data protection act  The consumer privacy act  European Privacy Regulations  
 The Gramm-Leach-Bliley act

You gave an incorrect answer, please try again!

### Question 2

During the study, you will be able to ...

- Pause and replay the videos  Leave at any point you want  Mute the videos  
 Refresh the browser anytime

You gave an incorrect answer, please try again!

Next

## Do you know Telenor?

Before you continue to the videos, we would like to know whether you have ever heard of the brand Telenor prior to this study?

- Yes  No

Next

### Privacy Reminder

For this video, your personal data will be handled as described in the consent form.

[Continue watching the video](#)

### Privacy Reminder

For this video, your personal data will be handled as described in the consent form.

[Continue watching the video](#)

The second video will start in a few seconds.

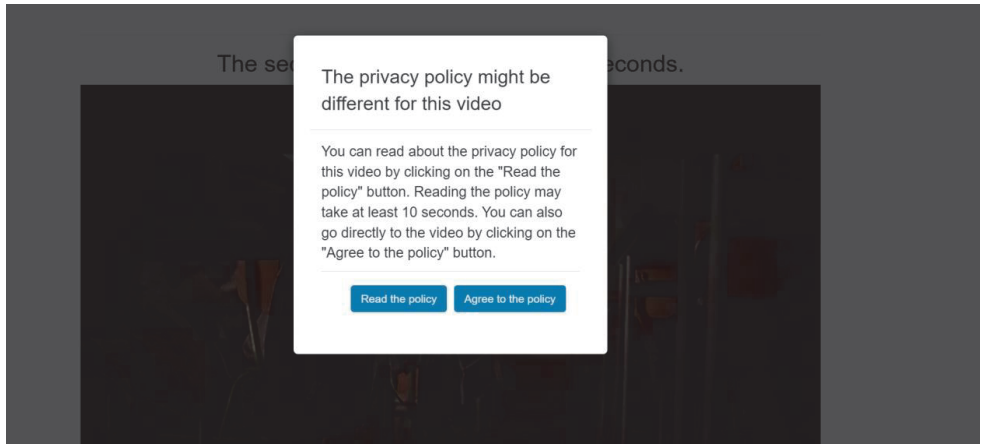


The se... seconds.

The privacy policy might be different for this video

You can read about the privacy policy for this video by clicking on the "Read the policy" button. Reading the policy may take at least 30 seconds. You can also go directly to the video by clicking on the "Agree to the policy" button.

[Read the policy](#) [Agree to the policy](#)

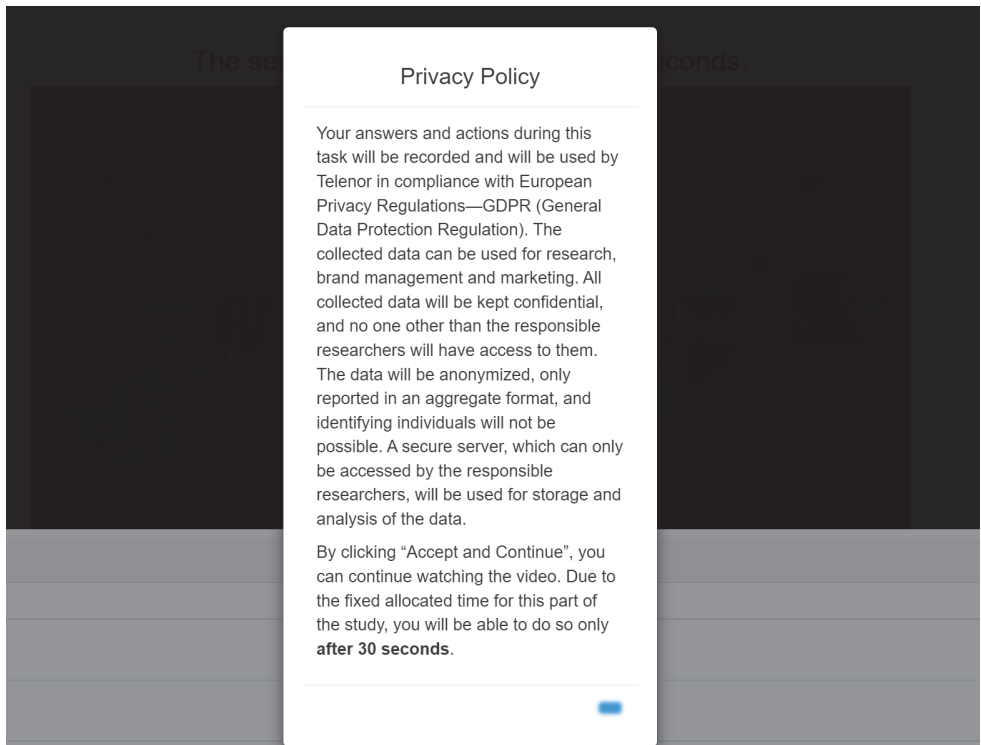


### The privacy policy might be different for this video

You can read about the privacy policy for this video by clicking on the "Read the policy" button. Reading the policy may take at least 10 seconds. You can also go directly to the video by clicking on the "Agree to the policy" button.

Read the policy

Agree to the policy



### Privacy Policy

Your answers and actions during this task will be recorded and will be used by Telenor in compliance with European Privacy Regulations—GDPR (General Data Protection Regulation). The collected data can be used for research, brand management and marketing. All collected data will be kept confidential, and no one other than the responsible researchers will have access to them. The data will be anonymized, only reported in an aggregate format, and identifying individuals will not be possible. A secure server, which can only be accessed by the responsible researchers, will be used for storage and analysis of the data.


By clicking "Accept and Continue", you can continue watching the video. Due to the fixed allocated time for this part of the study, you will be able to do so only **after 30 seconds.**

The se ... onds.

### Privacy Policy

Your answers and actions during this task will be recorded and will be used by Telenor in compliance with European Privacy Regulations—GDPR (General Data Protection Regulation). The collected data can be used for research, brand management and marketing. All collected data will be kept confidential, and no one other than the responsible researchers will have access to them. The data will be anonymized, only reported in an aggregate format, and identifying individuals will not be possible. A secure server, which can only be accessed by the responsible researchers, will be used for storage and analysis of the data.

By clicking “Accept and Continue”, you can continue watching the video. Due to the fixed allocated time for this part of the study, you will be able to do so only **after 10 seconds**.




The se ... onds.

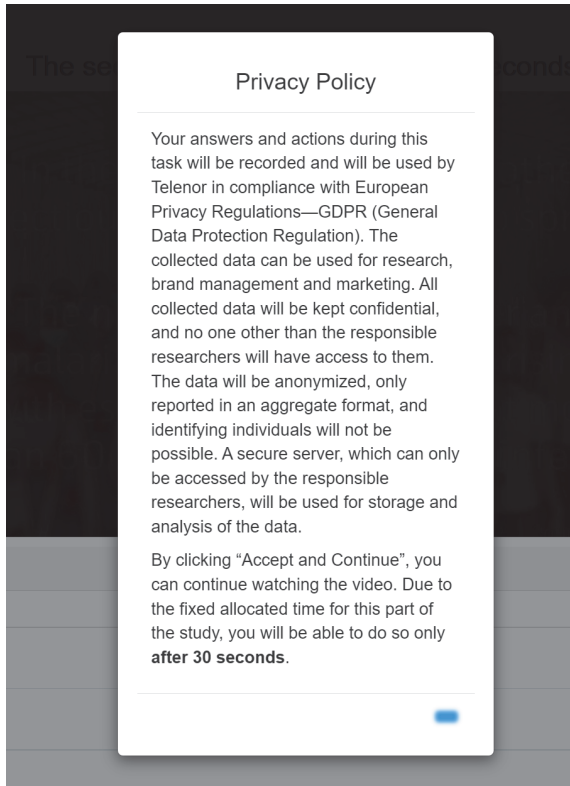
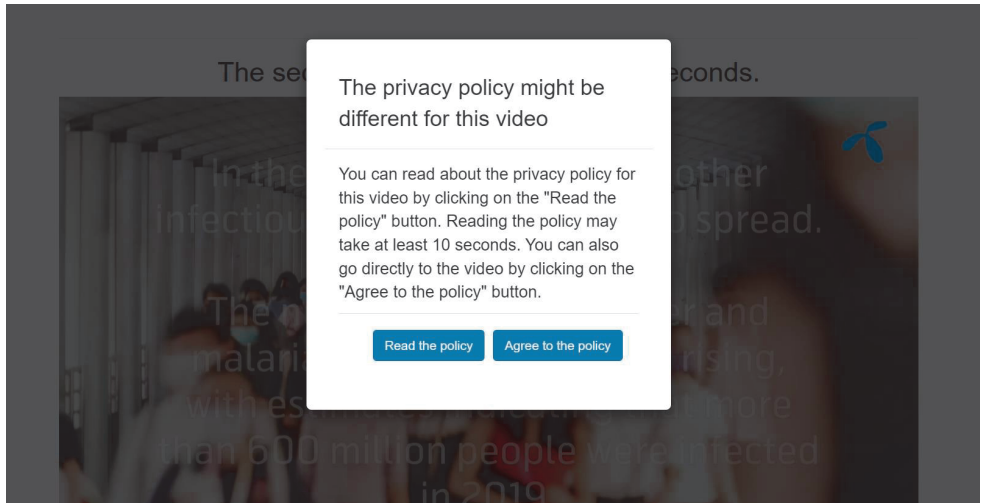
### The privacy policy might be different for this video

You can read about the privacy policy for this video by clicking on the “Read the policy” button. Reading the policy may take at least 30 seconds. You can also go directly to the video by clicking on the “Agree to the policy” button.

[Read the policy](#) [Agree to the policy](#)



In the ... other ... spread. ... and ... rising, ... more ... than 600 million people were infected in 2019



The se... seconds

### Privacy Policy

Your answers and actions during this task will be recorded and will be used by Telenor in compliance with European Privacy Regulations—GDPR (General Data Protection Regulation). The collected data can be used for research, brand management and marketing. All collected data will be kept confidential, and no one other than the responsible researchers will have access to them. The data will be anonymized, only reported in an aggregate format, and identifying individuals will not be possible. A secure server, which can only be accessed by the responsible researchers, will be used for storage and analysis of the data.

By clicking "Accept and Continue", you can continue watching the video. Due to the fixed allocated time for this part of the study, you will be able to do so only **after 10 seconds**.

[Next](#)

## Thank you for watching the videos!

In the next pages, you will be asked a few questions about the two videos you have watched.

After answering these questions, you will be given a link to submit your work.

Please click "**Next**" to go to the next page.

[Next](#)



## Questions about the content of the videos

Please read the two questions below carefully and answer separately for each video.

If you do not answer both questions correctly, you will not be allowed to finish the task.

### Video 1

What was the main character of the first video that you watched?

- A superhero    A boy    An elephant

### Video 2

What was the main character of the second video that you watched?

- A dog    A teacher    A girl

Next page

## Questions about the content of the videos

Please read the two questions below carefully and answer separately for each video.

If you do not answer both questions correctly, you will not be allowed to finish the task.

### Video 1

What was the main topic of the first video that you watched?

- Online recipes    Cyberbullying    Smart city planning

### Video 2

What was the main topic of the second video that you watched?

- Use of household tools    Population growth    Disease control

Next page

Please fix the errors.

## Questions about the content of the videos

Please read the two questions below carefully and answer separately for each video.

If you do not answer both questions correctly, you will not be allowed to finish the task.

### Video 1

What was the main character of the first video that you watched?

- A superhero  A boy  An elephant

### Video 2

What was the main character of the second video that you watched?

- A dog  A teacher  A girl

Wrong answer!

Next page

Please fix the errors.

## Questions about the content of the videos

Please read the two questions below carefully and answer separately for each video.

If you do not answer both questions correctly, you will not be allowed to finish the task.

### Video 1

What was the main topic of the first video that you watched?

- Online recipes  Cyberbullying  Smart city planning

Wrong answer!

### Video 2

What was the main topic of the second video that you watched?

- Use of household tools  Population growth  Disease control

Wrong answer!

Next page

## How much did you enjoy the videos?

### The video with the boy

On a scale from 1 to 5, did you enjoy watching this video?

1- Not at all  2  3  4  5- Very much

### The video with the girl

On a scale from 1 to 5, did you enjoy watching this video?

1-Not at all  2  3  4  5- Very much

Next page

## How much did you enjoy the videos?

### The video about cyberbullying

On a scale from 1 to 5, did you enjoy watching this video?

1- Not at all  2  3  4  5- Very much

### The video about disease control

On a scale from 1 to 5, did you enjoy watching this video?

1-Not at all  2  3  4  5- Very much

Next page

## Your chance to earn a bonus payment

**Answering the following question will give you the chance to earn a bonus payment. If your answer is in the range  $\pm 10$  of the correct answer, you will earn an extra 0.1 GBP.**

Out of every 100 people who participated in this study, how many people answered that they enjoyed watching the video with the boy in the question on the previous page (i.e. the two highest levels, 4 and 5)?



Next page

## Question about the privacy pop-up

When you saw the pop-up message about a potential change in the privacy policy, how did you think reading the privacy policy would affect your experience of watching the second video?

- Very negatively  Negatively  No effect  Positively  Very positively  I do not know

Next page

## Questions about your attitudes

**Please state the extent to which you agree or disagree with the following statements.**

I am concerned that online companies are collecting too much personal information about me.

- Strongly disagree  Disagree  Neither agree nor disagree  Agree  Strongly agree

I see myself as someone who takes risk.

- Strongly disagree  Disagree  Neither agree nor disagree  Agree  Strongly agree

Next page

## Your impression about Telenor after watching the videos

Do you agree or disagree that Telenor can be considered as a trustworthy company?

- Strongly disagree  Disagree  Neither agree nor disagree  Agree  Strongly agree

After watching the videos, would you be able to recognize the Telenor brand if you see it again?

- Yes  No

Would you consider buying a product from Telenor if it was available in your market?

- Definitely no  Probably no  Neither yes nor no  Probably yes  Definitely yes

What is your general impression about Telenor after watching these videos?

- Very negative  Negative  Neither negative nor positive  Positive  Very positive

Next page

## Some demographic information about you

What is your age?

What is your gender?

Male  Female  Other

[Next page](#)

## Question about your payment

Lastly, we are going to ask you to choose an option to receive your payment.

You have two options for receiving your payment. You can receive the payment, as it is calculated based on your answers right now, in 3 days. Otherwise, you can choose to receive the payment with a **0.05 GBP extra** with a 20 days delay.

Please decide which of the two options you would like to choose. You will receive your payment accordingly.

- Receive the payment in 3 days as it is calculated based on your answers
- Receive the payment with a 20 days delay with 0.05 GBP extra

[Next page](#)

## We would love to have your comments!

Any comments:

After writing any comments you may have, please continue to the next page to submit your work on Prolific.

[Next page](#)

## Thank you!

Thank you for your participation! To submit your work on Prolific, please click the link below.

[Submit](#)



## **Appendix: Paper 1 - English translation**





***This is a translated version of:***

Wasenden, O. C. (2020). Digitalt personvern – kunnskap, bekymring og adferd, *Magma* (2), 64 - 73

## DIGITAL PRIVACY – KNOWLEDGE, CONCERN AND BEHAVIOUR

*Author: Ole Christian Wasenden, Senior Researcher with Telenor and Industrial PhD candidate at the School of Economics and Business, NMBU.*

*Ole Christian Wasenden is an economist from UiO. He works at Telenor Research, primarily on competitive strategies and customer understanding. In 2018, he also became affiliated to the School of Economics and Business at NMBU as an Industrial PhD candidate, with digital privacy as his research topic.*

*Email: ole-christian.wasenden@telenor.com*

### Abstract

The amount of personal data generated through the use of digital services is ever-increasing. The aim of this article is to contribute to a better understanding of privacy from a customer perspective. Knowledge of data protection regulations and an understanding of consumers' privacy limits will be key competencies for business and industry in the years ahead. Companies must comply with the regulations, while also striking a balance between customers' privacy needs and their desire for personalised services.

In the summer 2017, we conducted a survey among young Norwegian consumers to assess their awareness of digital privacy, measured through levels of concern and knowledge. We then looked at how this awareness affected privacy behaviour. In spring 2018, the introduction of the EU's new General Data Protection Regulation (GDPR) and what was referred to as the 'Cambridge Analytic scandal' received a lot of media attention. To see whether this led to changes in privacy awareness, we conducted a new survey in 2018.

We find that young adults are aware of digital privacy. Their level of concern is high. Their level of knowledge was not as high, but it increased significantly from 2017 to 2018. A large proportion also take active steps to protect their data. What is known as the privacy paradox, i.e. that users are concerned but do nothing about it, receives little support in our data.

Companies that plan to use personal data must understand and adapt to these knowledgeable and concerned customers. In that way, privacy and careful use of personal data can become a competitive advantage rather than a legal challenge.

### Introduction

Many companies use personal data in their service development and customer care, and would like to offer personalised services that are as good as Amazon's book recommendations. They are often relevant, and you understand why they pop up and what data they are based on. Customers appreciate that personal data are used to create good, effective services, but the use of data should not be too invasive. If a company crosses the line into the private sphere, that may have a negative impact on customers' trust. Striking a balance between personalised services and protection of privacy is difficult, and for businesses there is risk on both sides. Too little use of personal data can result in competitors providing better services and winning customers. Too much use of data can be seen as an invasion of privacy and cause customers to switch suppliers. To be able to manage this two-sided

risk, it is important to understand customers' preferences and attitudes relating to the use of personal data. The aim of this article is to provide insight about young Norwegian consumers and to present an analytical framework and concrete examples from Norway.

The prevalence of smartphones and fast mobile computer networks has taken privacy issues into a new era. The private sphere becomes narrower when your phone is full of apps that log your activity. The intention is often good, and the information is used to develop good products and services. At the same time, however, this represents a potential threat to privacy, and users are concerned that data could end up in the wrong hands and be misused. It is argued that we are facing a privacy paradox, where consumers are concerned, but do nothing to protect their data (Kokolakis, 2017).

Two privacy-related incidents in spring 2018 received wide coverage in Norwegian media (see Figure 1): the Cambridge Analytica scandal and the introduction of the EU's new General Data Protection Regulation (GDPR). The media coverage highlighted two key issues relating to how personal data are used in digital markets. The news stories on Cambridge Analytica showed how data can be misused, while the GDPR stories showed how new regulations are intended to prevent this from happening.

The core of the Cambridge Analytica scandal was that Facebook data from around 87 million people, mainly in the USA, were used to influence people politically without their knowledge (Isaak & Hanna, 2018 and Tjøstheim & Høibø, 2019). Cambridge Analytica used personal data for purposes they had not communicated. The company also collected data from users they had no contact with. The data were used to predict personality, which many people would consider highly personal information. One of the outcomes of the scandal was a demand for more stringent regulation in the USA (Isaak & Hanna, 2018).

A new regulatory framework for data protection was introduced in the EU and Norway in May 2018. The framework, known as GDPR, is intended to strengthen EU citizens' right to data protection and privacy in an increasingly data-driven society. For a more detailed review of GDPR, see, e.g., Jarbekk and Sommerfeldt (2019).

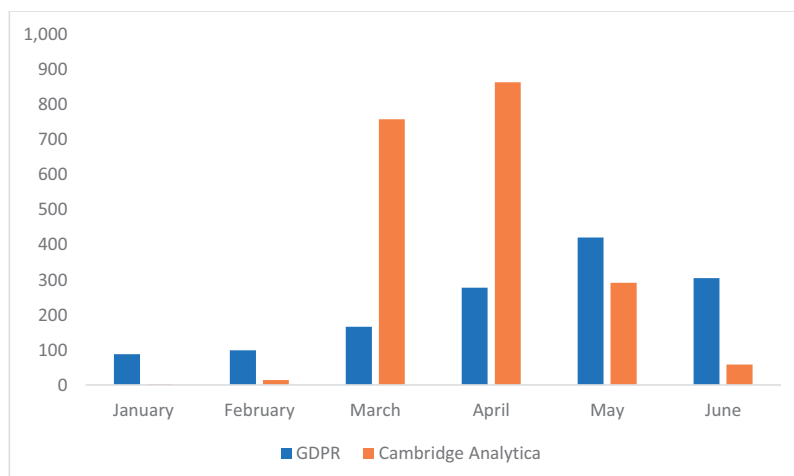


Figure 1 Number of Norwegian media stories on GDPR and Cambridge Analytica in spring 2018. Source: Retriever

This article is intended to contribute to a better understanding of privacy from a customer perspective. Do young Norwegians act in accordance with the privacy paradox? Are customers aware of and active

in relation to digital privacy? How can a commercial enterprise approach the issue? Greater knowledge about customers' relationship to privacy will enable companies to make better decisions when it comes to utilising customer data.

## Literature review

The literature on privacy is rich, and we will briefly cover three different sub-topics of importance to our study: (1) privacy awareness, measured by level of concern and knowledge, (2) behaviour, relating to both sharing of data and protection of own data, and (3) what is known as the privacy paradox. An overview of how personal data are used commercially in selected industries in Norway is available in Dulsrud and Alfnes (2017).

### *Privacy awareness*

Many studies use level of concern as the only measure of privacy awareness. Based on their level of concern, consumers are often divided into *fundamentalists*, *pragmatists* and *the unconcerned*. This segmentation was introduced by Alan Westin in 1995 (Westin, 2003). Since 1978, Westin has conducted a number of privacy surveys and indexed and studied the development of, among other things, the level of privacy concern. Kumaragura and Cranor (2005) have conducted a systematic review of Westin's work. Kobsa, Cho and Knijnenburg (2016) further develop the measurement of privacy concern in a digital context.

Level of knowledge is an important complement to concern. Park (2011) divides privacy knowledge into three parts: knowledge of the technical aspects of the internet, knowledge about how internet companies collect and use personal data, and knowledge of policymaking relating to privacy. Park and Jang (2014) also include what consumers are actively able to do to protect their data. Trepte et al. (2015) add knowledge about privacy risks and threats, and how such threats should be addressed.

Evjemo et al.<sup>1</sup> (under publication) combine levels of knowledge and concern in a privacy awareness matrix; see Figure 2. It divides consumers into *the unaware*, *the concerned*, *the unconcerned* and *the knowledgeably concerned*. Concern is measured through six statements, primarily based on Kobsa et al. (2016). Knowledge is measured through nine factual questions about privacy, partly based on Trepte et al. (2015) and Park and Jang (2014). We use the awareness matrix in our analysis and will return to this in the methodology section.

---

<sup>1</sup> Evjemo et al. (under publication) use the same 2017 dataset that we use in this study. They studied effects across countries, while we carry out deeper analyses of Norway and look at changes from 2017 to 2018.

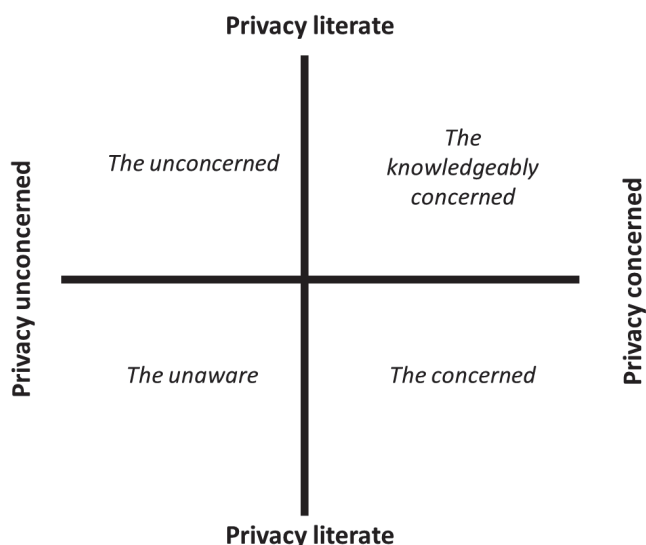


Figure 2 Privacy awareness matrix

Several studies also look at the driving forces that shape privacy awareness. A frequently used parameter is how a company presents its privacy settings (see, e.g., Tsai et al., 2011). We are not aware of studies that investigate the effects of media coverage on privacy awareness. However, the relationship between media coverage, knowledge and behaviour is well established in, for example, political economy. Prat and Strömberg (2013) describe how media coverage and media consumption increase insight into political issues, and how that, in turn, influences voting behaviour.

### Behaviour

Previous empirical studies of topics of importance to our work are reviewed in an article by Acquisti, Brandimarte and Loewenstein (2015). They summarise existing research along three dimensions. The first is uncertainty relating to the consequences of sharing data. It is unclear to consumers what the data are used for and it is difficult for them to put a value on possible negative consequences. Secondly, the perception of where the boundary lies between the private and the public is context-dependent. Thirdly, the factors that influence the level of concern and behaviour linked to privacy are manipulable. For example, different website designs can lead to a question being answered in different ways (John, Acquisti & Loewenstein, 2011). Many consumers have limited knowledge about these topics, while a commercial operator often has in-depth knowledge of how to encourage data sharing.

An experiment conducted among German users of a website (Utz et al., 2019) shows how easily behaviour can be influenced. The participants in the experiment were given different variants of a banner to accept cookies. Simple use of what is known as ‘nudging’ (Thaler & Sunstein, 2009), where the design nudges the user in a certain direction, clearly affected behaviour. For example, the acceptance rate increased from 39.2 to 50.8 per cent when the acceptance button went from being grey to being clearly highlighted. A study of how the introduction of GDPR affected Norwegian consumers can be found in Berg and Dulsrud (2018).

Wills and Zeljkovic (2011) study specific actions to protect one's own data, such as deleting cookies, using private browsing mode and deleting browser history. Questions about these types of actions are also used in surveys on knowledge levels. A Norwegian study conducted by Brandtzaeg, Pultier and Moen (2019) finds that more than half of the respondents have more than once refrained from downloading or using an app, because it requests access to information the user does not want to share.

### *The privacy paradox*

The concept of the privacy paradox, linked to the sharing of personal data online, was introduced in the early 2000s. Barnes (2006) uses the privacy paradox to describe how young people share information about themselves on social networks, and are then surprised to learn that their parents read it. The term is used differently today, however, and the paradox predicts that users of digital services have a high level of concern about privacy, but do little about it. Athey, Catalini and Tucker (2017) show that concerned consumers are willing to share personal data in return for a low monetary reward. A literature review conducted by Kokolakis (2017) finds that there is no consensus on the existence of the privacy paradox.

### Framework and hypotheses

In summer 2017, Telenor Research conducted a survey among young adults in Norway. The survey focused on the relationship between privacy awareness and behaviour aimed at protecting personal data. In spring 2018, the privacy issue received widespread media attention through the Cambridge Analytica scandal and the introduction of GDPR. This offered an opportunity to look for changes, which was why a new survey was conducted in 2018.

Based on existing literature, we have set up the framework given in Figure 3. Media coverage of privacy-related issues could affect privacy awareness. Here, we have drawn inspiration from political economy. Furthermore, privacy awareness will have an impact on behaviour, and this relationship is described in the literature. Studies of the privacy paradox specifically look at the relationship between concern and behaviour.



*Figure 3 Conceptual framework for connections between media coverage, awareness and actions*

Our data provide a limited basis for identifying a causal connection between media coverage and privacy awareness. We observed privacy awareness before and after the media coverage, but have no control group or randomisation. In addition to the sequence of the observations and the media coverage, we will rely on previous literature. It suggests that high media coverage of a topic results in increased knowledge among the population (see Prat and Strömberg, 2013). The assumed correlation between media coverage and level of concern is slightly more complicated and will probably depend on the content of the media coverage. Coverage of the Cambridge Analytica scandal will probably

have a negative impact and make people more concerned, while GDPR coverage will probably be positive. We will therefore not formulate hypotheses for the first stage of the framework, but will discuss developments in privacy awareness from 2017 to 2018 based on the increased media coverage.

For the second stage of the framework, we formulate three research hypotheses that look at the relationship between awareness and behaviour, and at the privacy paradox:

- H1: Concern about digital privacy is positively correlated with activity to protect personal data.
- H2: The level of knowledge about privacy is positively correlated with activity to protect personal data.
- H3: Young adults take active steps to protect their personal data.

## Methodology

### Sample and surveys

Based on questionnaire surveys conducted in 2017 and 2018, we look at Norwegian consumers in the 16 to 35 age group. In both cases, the data collection was carried out by Kantar TNS on behalf of Telenor Research. In both surveys, the respondents are drawn from Kantar’s web panel, with the goal of achieving comparable samples. The 2017 sample consists of 838 respondents, while the 2018 sample has 505.

Table 1 provides an overview of the age and gender of the respondents in the two samples. A non-parametric Kruskal-Wallis test shows no significant differences in age composition. A chi-square test shows significant differences in the gender distribution between the two surveys, with a predominance of women in the 2018 sample. We will therefore control for gender in the analyses.

*Table 1 Comparison of demographics in the 2017 and 2018 samples*

Demographics	2017 (N=838)	2018 (N=505)
Age		
16–20	12.29%	16.63%
21–25	24.58%	28.71%
26–30	37.59%	26.73%
31–35	25.54%	27.92%
Gender		
Women	46.78%	61.98%
Men	53.22%	38.02%

Note: age comparison  $\chi^2(1) = 1,38$ ;  $p = 0,24$ , gender distribution comparison  $\chi^2(1) = 29,20$ ;  $p = 0,00$

### *Indices for levels of concern and knowledge*

The measurement of privacy concern and knowledge is based on Evjemo et al. (under publication). Table 2 shows the five statements used to measure privacy concern.<sup>2</sup> The respondents indicated how

<sup>2</sup> The statements have a Cronbach’s alpha of 0.84, which indicates that they largely measure the same underlying concept.

much they agreed with the statements on a five-point Likert scale from ‘Strongly agree’ to ‘Strongly disagree’. We will assign each respondent an index score based on their answers to the five questions.<sup>3</sup> When we sum up the answers, the five answer categories result in a score ranging from minus two for very unconcerned to two for very concerned. We categorise a respondent as ‘concerned’ if she achieves a total score of two or higher.

*Table 2 Statements relating to concern*

<b>Statements used for the concern index</b>
I’m concerned that internet-based companies are collecting too much personal information about me
It bothers me that I can’t control how my personal information is used by internet-based companies
It usually bothers me when mobile apps ask me for personal information
I think mobile apps ask for more personal information than is necessary for the purpose of the app
It bothers me that personal information provided to an internet-based company for a particular purpose may be used for other purposes

The knowledge index is based on nine statements that are either true or false. The statements are reproduced in Table 3.<sup>4</sup> Also here, the respondents were given five answer options from ‘Definitely true’ to ‘Definitely false’. When we sum up the answers, the respondents are given a score of minus two if they have answered ‘Definitely true’ and the statement is false. Correspondingly, they are given a score of two if they have answered ‘Definitely true’ and the statement is true. In the same way as in Evjemo et al., we classify a respondent as ‘knowledgeable’ if she achieves a total score of nine or higher.

*Table 3 Knowledge statements*

<b>Knowledge statements</b>
Facebook, Google and similar companies track your activity online
Many mobile apps register your location
Social network operators such as Facebook also collect information about people who don’t use Facebook
When a mobile app has a privacy statement, it means personal data are not shared with other apps or companies

<sup>3</sup> We have chosen to omit one statement, despite the fact that it was used by Evjemo et al., because it is not unambiguous.

<sup>4</sup> The statements have a Cronbach’s alpha of 0.75, which indicates that they measure the same underlying concept to an acceptable degree.

Facebook, Google and similar companies delete personal data after a pre-defined period of time
Those who make apps only collect the personal information that is necessary for the service to work
When you deactivate GPS on your mobile phone, your location cannot be tracked
Your browser history will normally be stored on your mobile phone
It's not possible to hack private information from your mobile phone

In order to look at privacy-related actions, we asked the respondents whether they actively protect their personal data. Examples of such actions are to delete cookies and to turn off location tracking on your mobile phone. We asked about six actions, and the respondents were given the options 'more often than once a month', 'less often than once a month', 'never, because I don't see the need' and 'never, because I don't know how to'. This enables us to see whether the respondents are concerned and passive, i.e. act in accordance with the privacy paradox, or whether they take active steps to protect their privacy better.

## Results

Our findings support the three research hypotheses, and we can reject the associated null hypotheses that 1) concern about privacy is not positively correlated with activity to protect personal data, 2) the level of knowledge about privacy is not positively correlated with activity to protect personal data, and 3) young adults do not take active steps to protect their personal data. Our results also show a significant increase in knowledge about privacy, and a reduction in privacy concern, in the course of about six months. We cannot conclude that this is due to media coverage, but we find it likely that that is the cause. Factors that influence privacy awareness should be further investigated.

### *Changes in levels of knowledge and concern from 2017 to 2018*

Norwegians have an active relationship to digital privacy. The level of concern, measured using our index, was high in both 2017 and 2018, at around 84 to 79 per cent, respectively. In other words, we see a decrease, and the same is observed for both genders. The proportion with a high level of knowledge in 2017 was 42 per cent among women and 58 per cent among men. That increased to 48 and 72 per cent, respectively, in 2018, which means that an increase was observed for both genders, but that the levels are higher for men.

Table 4 shows the results of two regression analyses for the level of knowledge and concern, respectively, in which we take a closer look at the changes from 2017 to 2018, controlled for gender and age. In the first regression analysis, we only look at the effect of the time parameter, while in the second we control for gender and age. Both the increase in knowledge and the decrease in concern from 2017 to 2018 are significant, also when controlled for gender and age. Furthermore, we see that, in this age group (16 to 35), both knowledge of and concern about digital privacy increase significantly with age. Women have significantly lower digital privacy knowledge than men.



Table 4. Regression analyses – changes in levels of knowledge and concern

	(1) Level of knowledge	(2) Level of knowledge	(3) Level of concern	(4) Level of concern
Year	0.735* (0.291)	1.067*** (0.285)	-0.578** (0.213)	-0.562** (0.214)
Age		0.139*** (0.028)		0.091*** (0.021)
Woman		-1.869*** (0.283)		0.071 (0.212)
Constant	-1,455.9* (586.3)	-2,128.5*** (574.8)	1,170.6** (429.1)	1,135.7** (431.0)
N	1343	1343	1319	1319
adj. R <sup>2</sup>	0.004	0.063	0.005	0.018

Standard error in brackets, \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

Figure 4 illustrates how the respondents fall into the four segments in the awareness matrix created by Evjemo et al. (under publication), in 2017 and 2018, respectively. The proportion of *knowledgeable* respondents is higher in 2018 than in 2017, and the increase can be observed across both *the unconcerned* and the *knowledgeably concerned* segments. The biggest reduction from the 2017 to the 2018 survey can be seen in the group that was only concerned. It is worth noting that the clearly biggest group is the *knowledgeably concerned* segment. We will return to the significance of this when we now take a closer look at the relationship between privacy awareness and actions to protect personal data.

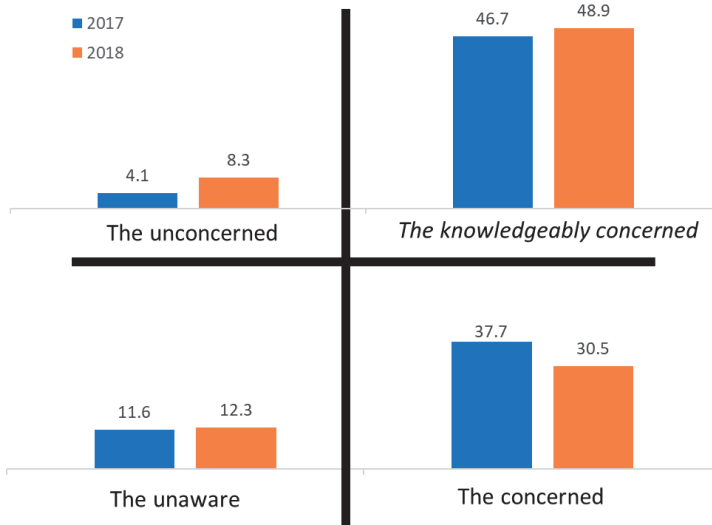


Figure 4 Awareness matrix – changes in the different segments from 2017 to 2018.

### Protection of personal data

The vast majority of young adults use one or more means to protect their data. In total across both surveys, only 5 per cent of respondents do nothing. In Table 5, we see, for example, that 40 per cent of respondents in this age group use a private tab when surfing the internet, at least once a month, while 33 per cent turn off location tracking as frequently.

Table 5 Proportion who perform the action more than once a month in the 16–35 age group, 2017 and 2018, N=1343

	In total	The unaware	The concerned	The un-concerned	The knowledgeably concerned
Delete browser history	24.8	19.2	23.7	17.1	28.1
Use private/incognito tab when browsing	40.1	26.6	29.7	51.3	49.6
Block cookies	21.1	9.7	15.1	18.4	28.6
Turn off the location function to avoid tracking	33.2	18.7	32.6	11.8	39.8
Use the browser version of a service instead of the app	26.4	13.9	21.5	20.0	33.6
Stop the installation of an app because you are asked to disclose too much personal data	18.8	9.6	17.6	4.0	23.6

Note: Combined data from both 2017 and 2018

Based on the six possible actions, we calculate a total level of activity between 0 and 12. When we sum up the actions, the respondents are assigned a score of two if they perform an action more than once a month, a score of one if they perform it less often than once a month, and zero if they do not perform the digital privacy action in question.

To examine the relationship between privacy actions and knowledge and concern, we present four regression analyses in Table 6, all based on data from both 2017 and 2018. The dependent variable is the total activity level. Model 1 only uses knowledge and concern as explanatory variables, and we find that both are significantly positive. Both increasing knowledge and increasing concern lead to a higher level of activity. Model 2 uses gender, age and year as explanatory variables, and we find that gender is significant. Women perform fewer privacy protective actions. The results from Models 1 and 2 still hold true when we merge the first two in Model 3. We find a positive effect of concern and knowledge, and that women have a lower level of activity than men, given the same levels of knowledge and concern. When, in Model 4, we include an interaction effect between knowledge and concern, we see that only gender and the interaction are positive. This means that, if you have both a high level of knowledge and a high level of concern, this results in a high level of activity to protect data. The individual components – knowledge and concern – are no longer significant.

In other words, it is the respondents in the ‘*knowledgeably concerned*’ segment, on the upper right of the awareness matrix, who really stand out from the others when it comes to protecting their data.

Table 6 Regression analysis – total level of activity for individual respondents across years as an independent variable

	(1) Level of activity	(2) Level of activity	(3) Level of activity	(4) Level of activity
Level of knowledge	0.101*** (0.016)		0.087*** (0.016)	0.034 (0.025)
Level of concern	0.238*** (0.0210)		0.238*** (0.021)	-0.0500 (0.103)
Woman		-0.881*** (0.163)	-0.756*** (0.154)	-0.735*** (0.154)
Age		0.042** (0.016)	0.009 (0.015)	0.008 (0.015)
Year		-0.263 (0.164)	-0.208 (0.155)	-0.187 (0.155)
Interaction between knowledge and concern				0.0109** (0.004)
Constant	1.577*** (0.398)	4.899*** (0.461)	2.187*** (0.559)	3.510*** (0.725)
<i>N</i>	1319	1343	1319	1319
adj. <i>R</i> <sup>2</sup>	0.158	0.034	0.176	0.181

Standard error in brackets, \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

## Discussion and summary

In the political debate, we have heard statements like ‘privacy is dead’. This is, for example, the message in an article published in Forbes (Morgan, 2014) with the heading ‘*Privacy Is Completely And Utterly Dead, And We Killed It*’. The main point of the Forbes article was that we surround ourselves with so many services that collect and store data that it is impossible to maintain digital privacy. This is obviously a simplification, but the claim forms a good backdrop to discussing our findings. If privacy is dead, you would think that the majority of young people today would be indifferent to it, which does not tally with our findings.

In our analysis, we have studied various aspects of young Norwegian adults’ attitudes to sharing personal data in a digital context. It is difficult to prevent your personal data from being collected and used by a number of players, as the ‘privacy is dead’ claim suggests. Our analysis suggests that the level of awareness is high, however. A very high proportion of respondents state that they are concerned about how their data are used, and more than half of the respondents have a high level of knowledge. We also find that many take active steps to protect their data.

### *Does privacy awareness change in a period of high media coverage?*

From 2017 to 2018, the proportion of knowledgeable respondents increased from 42 to 48 per cent among women and from 58 to 72 per cent among men. Over a relatively short period of a little more than six months, we know there was extensive media coverage of privacy issues. As described above,

we have not conducted a controlled experiment to study the effect of media coverage on privacy awareness. Based on research into such effects from other fields of research, however, we expected an increase in the level of knowledge. Our findings are in line with this expectation.

The level of concern was high in both 2017 and 2018. It was natural to assume that the Cambridge Analytica scandal would result in a further increase in concern, but the results show that the level decreased slightly. One possible reason may be the introduction of GDPR. When new and more stringent regulations are introduced that aim to prevent misuse of customer data, that could reduce our level of concern. A higher level of knowledge can also lead to a reduced level of concern. It is possible that consumers have gained enough knowledge to feel that they are in control.

#### *Active steps and the privacy paradox*

Our analyses indicate that many young adults take active steps to protect their data. We see that there are differences between the different types in the awareness matrix, however, and that the *knowledgeably concerned* do most. This group was clearly the biggest in both 2017 and 2018.

At the same time as consumers are concerned about their personal data, the vast majority use data-hungry services like Facebook and Google. This also applies to consumers with a high level of knowledge who use various methods to protect their data. It is likely that consumers weigh the costs against the benefits, and that services that are considered highly valuable are used despite being data-hungry. Services with a lower utility value are dropped for privacy reasons. It is difficult for consumers to predict potential future consequences of data that are collected today. For the same reason, it is difficult to weigh possible future consequences against the utility value, which often comes immediately. This is one of the main topics Acquisti et al. (2015) discuss in their review article.

We find no clear support for the privacy paradox in our analysis and believe that the concept, in some contexts, is used in a way that removes necessary nuances from the analyses. We believe future research should focus more directly on the process consumers undergo when deciding whether or not to use a data-hungry service. In our view, a better understanding of this decision-making process is more important than understanding the privacy paradox itself.

#### *Implications for businesses and public authorities*

A very high proportion of respondents are concerned about how their personal data are used. At the same time, the sample is divided when it comes to knowledge. This should be taken into account when designing policies and developing future commercial strategies.

Digitalisation will continue and so will the collection and use of personal data. To enable everyone to participate and get the maximum benefit from technology, possible measures to increase the level of knowledge and reduce the level of concern should be given a higher place on the political agenda.

For businesses, customers' attitudes to privacy can form the basis for a competitive advantage. GDPR requires customers to give their informed consent before personal data can be used, and this sets an absolute limit on companies' utilisation of personal data. It is possible, however, that consumers have other tolerance limits than those provided for in the regulations. Companies must therefore strive to understand their customers' privacy preferences and adapt to concerned and knowledgeable customers. Companies that succeed in providing the services customers want, without being invasive, could gain an advantage in the market.

Overall, we must conclude that privacy is not dead. In January 2020, a number of media outlets reported that Facebook planned to make it easier for users to control which data the company should use. This is one of many examples of privacy being taken seriously. With our findings, which

clearly show that privacy is something many people are concerned about, we wonder whether, in future, we might see more headlines along the lines of 'Privacy strikes back'.

## Literature references

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015, 30 January). Privacy and Human Behavior in the Age of Information. *Science*, 347 (6221), 509–14.
- Athey, S., Catalini, C. & Tucker, C. (2017). The Digital Privacy Paradox: Small money, Small Costs, Small Talk. *NBER Working Paper*, 23488.
- Barnes, S. B. (2006). A Privacy Paradox: Social Networking in the United States. *First Monday*, 11 (9).
- Berg, L., & Dulrud, A. (2018). Tillit og sårbarhet på nett. Forbrukernes praksiser og vurderinger etter innføringen av den nye personvernforordningen (GDPR) i Norge 2018. *SIFO Oppdragsrapport*. 9 – 2018.
- Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2019). Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy. *Social Science Computer Review*, 37(4), 466–488.
- Dulrud, A. & Alfnes, F. (2017). Når stordata blir Big Business. *SIFO Oppdragsrapport*. 10 – 2017.
- Evjemo, B., Grønnevet, G. Ling, R., Nag, W., Røhr, H. L., & Wasenden, O. C. (under publication). Privacy on Smartphones: A Cross-National Study. In Ling, R., Fortunati, L., Lim, S. S., Goggin, G. & Li, Y. (eds.) *The Oxford Handbook of Mobile Communication, Culture, and Information*, Oxford: Oxford University Press.
- Isaak, J. & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51 (8), 56–59.
- Jarbekk, E. & Sommerfeldt, S. (2019). *Personvern og GDPR i praksis*. Oslo: Gyldendal Damm Akademisk.
- John, L. K., Acquisti, A. & Loewenstein, G. (2011). Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information, *Journal of Consumer Research*, 37 (5), 858–873.
- Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors. An elaboration likelihood model approach. *Journal of the Association for Information Science and Technology*, 67 (11), 2587–2606.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134.
- Kumaragura, P. & Cranor, L. F. (2005). Privacy Indexes: A Survey of Westin's Studies. *Working paper CMU-ISRI-05-138*, Carnegie Mellon University.
- Morgan, J. (2014). Privacy Is Completely And Utterly Dead, And We Killed It. *Forbes*, retrieved from <https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/>
- Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, 40 (2), 215–236.
- Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, 38, 296–303.
- Prat, A., & Strömberg, D. (2013). The political economy of mass media. *Advances in economics and econometrics*, 2, 135.
- Thaler, R.H. & Sunstein, C.R. (2009). *Nudge: improving decisions about health, wealth and happiness*. London: Penguin Books.

- Tjøstheim, I. & Høibø, M. (2019) Nordmenn og deling av persondata. *Norwegian Computing Centre*, Report no 1044.
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fisher, M., Hennhøfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (eds.), *Reforming European data protection law*, (333–365). Heidelberg, Germany: Springer.
- Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research*, 22(2), 254–268.
- Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM Conference on Computer and Communications Security*. ACM Press, New York, NY, USA
- Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59 (2), 431–453
- Wills, C. & Zeljkovic, M. (2011), "A personalized approach to web privacy: awareness, attitudes and actions", *Information Management & Computer Security*, Vol. 19 No. 1, pp. 53–73.

## Ole Christian Wasenden



Ole Christian Wasenden has a master's degree in economics from the University of Oslo. He works at Telenor Research and Innovation. His PhD work has been done with an Industrial PhD grant from The Research Council of Norway.

Collection of personal data is omnipresent in today's digital life and privacy challenges are growing. When online, individuals must weigh what they gain from using services against the potential costs of loss of privacy. The thesis consists of four papers and examines the decision-making process and preferences relating to digital privacy.

The *first paper* studies attitudes towards privacy from a customer perspective through a two-way survey conducted among young Norwegians. In the *second paper*, the willingness of young mobile users in Norway, Serbia, Malaysia, and Pakistan to share personal data in return for receiving personalized ads on their cell phones is investigated. The *third paper* explores attitudes towards sharing personal data for combating contagious diseases. A two-wave survey conducted in Norway and Sweden analyzes the impact of personal characteristics and information on privacy attitudes. The *fourth paper* investigates whether people avoid information about privacy when they are exposed to highly entertaining online content, through an online experiment.

This thesis contributes new insights into privacy, human behavior and the sharing of personal data in digital everyday life. In the thesis, this topic is illuminated from very different angles. On one hand, we have the commercial personalized ads service where the benefit is reaped by the individual, and, on the other, how personal data can be used to combat an infectious disease with benefits at the societal level. The data are collected in countries that are very different in terms of both their technological and economic development, and in relation to attitudes to privacy and its status in law. Despite these differences, there are similarities that recur in all four articles. Firstly, we see that a large proportion of respondents are concerned about their privacy when online. Furthermore, high levels of concern are accompanied by lower willingness to share data, while the opposite is the case for trust in the actor who collects the data. Our findings pave the way for more research on privacy and human behavior.

School of Economics and Business  
Norwegian University of  
Life Sciences (NMBU)  
P.O Box 5003  
N-1432 Ås, Norway

Telephone: +47 99 24 40 20  
e-mail: [olwa@nmbu.no](mailto:olwa@nmbu.no)

ISSN: 1894-6402  
ISBN: 978-82-575-2055-7

Professor Frode Alfnes at NMBU was Ole Christian's main supervisor and Eleonora Freddi was his main internal supervisor at Telenor.

E-mail: [olewas@gmail.com](mailto:olewas@gmail.com)





ISBN: 978-82-575-2055-7

ISSN: 1894-6402



Norwegian University  
of Life Sciences

Postboks 5003  
NO-1432 Ås, Norway  
+47 67 23 00 00  
[www.nmbu.no](http://www.nmbu.no)