

Master's thesis

Irina Gundersen

Privacy Management and Preservation in the Era of Targeted Advertising

Master's thesis in Communication Technology

Supervisor: Katrien De Moor

June 2022

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication
Technology



Norwegian University of
Science and Technology

Irina Gundersen

Privacy Management and Preservation in the Era of Targeted Advertising

Master's thesis in Communication Technology
Supervisor: Katrien De Moor
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Title: Privacy Management and Preservation in
the Era of Targeted advertising

Student: Irina Gundersen

Problem description:

Targeted advertisement is a large part of the Internet economy. This form of advertising aims to appeal directly to the consumers who are most likely to respond to the relevant product. Large advertising networks collect and analyze data all over the Internet, in order to sell to advertisers wishing to reach their desired audiences. In this system, the end-user may feel powerless when tasked with taking control over their data. There have been developments in the past few years where lawmakers have tried to give some power back to the consumers, for instance with The General Data Protection Regulation in Europe in 2018. However, consumers might still not have the desired level of privacy, either because they do not know how to achieve it or they are unable to because of technological constraints. Many previous studies have focused on the management of privacy settings on Social Networking Sites (SNS), where the settings mostly focus on who has access to the posts. However, there have been few studies focusing on the privacy management of a broader data collection in relation to targeted advertising.

This thesis aims to map the privacy concerns and attitudes of users towards personal data sharing and privacy management in the context of targeted advertising, as well as to investigate which strategies are used by users to protect their information and explore what the biggest hurdles are to do so. This will be done by combining different types of data, both with an online survey as well as a qualitative component.

Date approved: 2022-02-11

Responsible professor: Katrien De Moor, NTNU, IIK

Supervisor(s): Katrien De Moor, NTNU, IIK

Abstract

Internet users' daily lives are influenced by data collection and targeted advertising, yet it is still something most people have little knowledge of and control over. Considering the influence targeted advertising can have over people's lives, both in the impact of product placements and politically targeted advertising, there should be options available for those wishing for greater control over their data. Previous research has, among other things, focused on what influences privacy behavior and the factors that matter in privacy management. This thesis aims to research what relationship users have to their privacy and privacy management, which strategies they employ in their daily lives, and lastly, how manageable settings for privacy and targeted advertising are for the users of central online platforms.

These aspects are researched by combining an online survey with 128 respondents with a user experiment in a mixed-method approach with 20 participants. From this, it is clear that it is difficult for the average user to manage their privacy in a meaningful way because of how difficult it is and appears. Because of this, some have given up managing their privacy, as they feel their efforts do not matter or do not have the required skills. Although most make some effort to protect their privacy, the research in this thesis also found that users might overestimate their ability to do so. Thus, users might set themselves in situations where they do not have the protection they think they have. Additionally, this research also suggests that there might be differences between different groups in how well they can make the changes they wish to make. The implications of this research indicate a discrepancy between the privacy users want to achieve and the privacy they, in reality, have, causing large amounts of data to be collected without many people being able to choose who has their data and for what it is used.

Sammendrag

Livet til internettbrukere blir daglig påvirket av datainnsamling og målrettet reklame, men dette er fortsatt noe de fleste har lite kunnskap og kontroll over. Sett påvirkningskraften målrettet reklame kan ha over livene til folk, ikke bare med tanke på produktplassering, men også politisk målrettet reklame, burde det finnes muligheter for at folk kan øke kontrollen over informasjonen sin. Tidligere forskning har blant annet fokusert på hva som påvirker hvordan man oppfører seg rundt personvern, samt hvordan grensesnitt kan påvirke personvernshåndtering. Denne oppgaven undersøker hva slags forhold folk har til personvern og personvernshåndtering, hvilke strategier folk bruker for å håndtere personvernet sitt, og hvor lett det er for brukere å håndtere innstillinger relatert til personvern og målrettet reklame på sentrale tjenester på nettet.

Disse aspektene ble undersøkt ved å kombinere en spørreundersøkelse med 128 deltakere og et brukerekspériment i en tilnærming med blandede metoder med 20 deltakere. Fra denne forskningen er det klart at det er vanskelig for vanlige brukere å håndtere personvern på en meningsfull måte, på grunn av hvor vanskelig det er og framstår. På grunn av dette, er det enkelte som har gitt opp å håndtere personvernet sitt, da de enten føler at tiltakene de gjør ikke har noe å si, eller føler at de ikke har kompetansen som kreves. Selv om de aller fleste gjør en innsats for å beskytte personvernet sitt, viser undersøkelsene fra denne oppgaven at brukere har en tendens til å overvurdere hvorvidt de klarer å gjøre de endringene de tenker at de gjør. Dermed kan det være brukere setter seg selv i situasjoner der de ikke har den beskyttelsen de selv tenker at de har. I tillegg antyder undersøkelsene at det er forskjeller mellom hvordan ulike grupper klarer å gjøre de endringene de selv ønsker. Resultatene fra undersøkelsen kan tyde på at det er en forskjell mellom det personvernet folk har og det personvernet folk skulle ønske at de hadde. Dette fører til at store mengder data samles uten at man har muligheten til å velge hvem som har tilgang til dataen og hva det brukes til.

Preface

This thesis is the final submission for the MSc. in Communication Technology and Digital Security at the Norwegian University of Science and Technology (NTNU). The supervisor for this thesis has been Associate Professor Katrien De Moor from the Department of Information Security and Communication Technology (IIK) at NTNU. This work is the continuation of the preliminary study from TTM4502 and was conducted in the spring of 2022.

Acknowledgements

I would like to thank my supervisor Katrien De Moor for her invaluable guidance and support throughout this project. She has been a great motivator to make this thesis as great as possible and kept me excited to continue working on this project until the very end.

Additionally, I owe a great thanks to the girls in my master's office for great conversation, support, and many laughs over the past few months. Without them, I am sure the writing process would not have been as much fun.

Contents

List of Figures	xiii
List of Tables	xv
List of Acronyms	xvii
1 Introduction	1
1.1 Research Questions	4
2 Background	7
2.1 Behind Data Collection and Targeted Advertising	7
2.1.1 How Does Targeted Advertising Work?	7
2.1.2 What Is Targeted Advertising Worth?	10
2.2 The User Perspective of Privacy Management	11
2.2.1 The Psychology of Users	11
2.2.2 False Sense of Security	13
2.2.3 The Privacy Paradox	14
2.2.4 Achieving Desired Levels of Privacy	14
2.2.5 The Importance of Privacy Management	14
2.2.6 What Can be Done to Change the Privacy Imbalance?	15
2.3 General Data Protection Regulation	16
2.3.1 Changes in Privacy After the GDPR	17
3 Related work	19
3.1 Large Scale Surveys	19
3.1.1 What Makes Users Share their Information with Advertisers?	19
3.1.2 What Affects Users Attitudes Towards Privacy Policies?	20
3.1.3 How do Users Interpret Technical Terms in Privacy Policies?	21
3.1.4 What Role Does Privacy Fatigue Play in Privacy Management?	21
3.1.5 How do Privacy Concerns and Self-Efficacy Influence Privacy	
Management?	22
3.1.6 Privacy Attitudes in Norway	22
3.2 User Experiments	23

3.2.1	How Does the User Interface Affect Engagement with Privacy Features?	23
3.2.2	What Value do Customers Place on Their Personal Data? . .	24
3.2.3	How Willing Are Users to Sell their Personal Data?	24
3.2.4	How Does Targeted Advertising Compare to Non-Targeted Advertising?	25
4	Methodology	27
4.1	Online Survey	27
4.1.1	Question Selection	28
4.1.2	Quality Assurance	30
4.1.3	Distribution	30
4.2	User Experiment and Interview	31
4.2.1	The Setup	31
4.2.2	Creating "Ragnhild Paulsen"	32
4.2.3	Tasks and Goals	33
4.2.4	Accessing the Settings	42
4.2.5	Conducting the User Experiment and Interview	46
4.2.6	Grading	46
4.2.7	Anonymity and Privacy	47
4.2.8	Limitations	48
4.3	Analysis	48
4.3.1	Online Survey	48
4.3.2	User experiment and interview	48
5	Results	49
5.1	Survey	49
5.1.1	Demography	49
5.1.2	Questions on Terms	51
5.1.3	Targeted Advertising	55
5.1.4	Privacy	56
5.1.5	Privacy Focused Services	58
5.1.6	Willingness to Share Information with Advertisers	61
5.2	User Experiment	64
5.2.1	Correct answers and times	64
5.2.2	Participants	65
5.2.3	Differences Between the Participants	67
5.2.4	Accuracy of Self-Evaluation	69
5.2.5	User Perception	71
5.3	Interview	76
5.3.1	How Did They Feel Like it Went?	76
5.3.2	What Was the Most Difficult Aspect of the Tasks?	77

5.3.3	What Could Have Made it Easier	78
5.3.4	The User Interface	78
5.3.5	Familiarity with the Settings	79
5.3.6	Relationship with Online Privacy	80
5.3.7	Thoughts on Advertising and Data Collection	81
5.3.8	Strategies in Online Privacy Management	83
5.3.9	What Keeps Them from Protecting their Privacy?	85
5.3.10	What They Wish Existed	86
6	Discussion	89
6.1	RQ1: What Relationship do Users Have to Their Online Privacy and Privacy Management?	89
6.1.1	Issues to Privacy Management and Possible Solutions	93
6.2	RQ2: Which Strategies do Users Use to Control How Their Personal Data is Shared and Used	93
6.3	RQ3: To What Extent do Users Perceive the Privacy Settings of Different Services as Manageable?	95
6.3.1	Self-Evaluation vs Reality	97
6.4	Limitations	99
7	Conclusion and Future Work	101
7.1	Future Work	103
	References	105
	Appendices	
A	Online Survey	111
B	User Experiment	123
C	Interview Guide	133

List of Figures

2.1	A simplified explanation of how advertising spaces are bought and sold.	10
4.1	Facebook profile for Ragnhild Paulsen.	32
4.2	Settings for Task 1.	34
4.3	Settings for Task 2.	35
4.4	Settings for Task 3.	36
4.5	Settings for Task 4.	37
4.6	Settings for Task 5.	38
4.7	Settings for Task 6.	39
4.8	Settings for Task 7.	40
4.9	Settings for Task 8.	41
4.10	The relevant categories of Facebook settings.	42
4.11	Facebook ad preferences.	43
4.12	The correct categories of Facebook ad settings.	43
4.13	The correct Google settings under <i>Data and Privacy</i> .	44
4.14	Where to access the settings in Google Chrome.	44
4.15	Where to access the VG settings.	45
4.16	The setup for the user experiment.	47
5.1	Age groups of the respondents.	50
5.2	Gender of the respondents.	50
5.3	Education level of the respondents.	51
5.4	Nationality of respondents.	51
5.5	ICT-related background among respondents.	52
5.6	Correct and incorrect answers to knowledge questions.	52
5.7	Answers to where session data is stored in private browsing.	53
5.8	Answers to what third party cookies are.	54
5.9	Responses on password preferences.	54
5.10	Attitudes towards targeted advertising.	56
5.11	Responses on privacy attitudes.	58
5.12	How many of the respondents had heard of the different services.	59
5.13	How often the respondents used the different services.	60
5.14	Hurdles for using privacy-focused services.	61

5.15	Willingness to share information with advertisers.	62
5.16	Results from the user experiment.	65
5.17	The age, gender, and background of the participants.	66
5.18	The gender distribution of participants with and without an ICT back- ground.	66
5.19	The correct responses for each task with gender.	67
5.20	The correct responses for each task with relevant fields of study.	67
5.21	The correct responses with percentage for gender.	68
5.22	The correct responses with percentages for relevant fields of study.	69
5.23	The distribution of the response categories.	70
5.24	Correctness of self-evaluation for each task.	70
5.25	Correctness of self-evaluation for every participant.	71
5.26	The percentage of the responses given by the genders in the different categories.	72
5.27	The percentage of the response given by ICT and non-ICT participants for each category.	72
5.28	The responses to the claim: "The setting was easy to locate".	73
5.29	The responses to the claim: "The user interface was easy to use".	73
5.30	The responses to the claim: "I am happy with the amount of time I used to complete the task".	74
6.1	Summary the relationship users have to privacy and privacy management.	92
6.2	Summary of the strategies users have with privacy management.	95
6.3	Summary of how setting management was for the users.	98

List of Tables

4.1	Survey Questions with References	29
5.1	Summary of how they felt it went	76
5.2	Summary of what the participants found the most difficult	77
5.3	Summary of what the participants felt could have made the tasks easier	78
5.4	Summary of comments the participants made on the user interface.	78
5.5	Summary of the participants' relationship with online privacy	80
5.6	Summary of the participants' thoughts on advertising and data collection	81
5.7	Summary of the participants' privacy management strategies	83
5.8	Summary of the hurdles the participants face for better privacy protection	85
5.9	Summary of things the participants wished existed	86

List of Acronyms

2FA Two Factor Authentication.

AI Artificial Intelligence.

DMP Data Management Platform.

DSP Demand-Side Platform.

GDPR General Data Protection Regulation.

ICT Information and Communication Technology.

IIK Department of Information Security and Communication Technology.

NSD The Norwegian Centre for Research Data.

NTNU Norwegian University of Science and Technology.

PETs Privacy Enhancing Technologies.

PII Personally Identifiable Information.

RTB Real-Time Bidding.

SNS Social Networking Site.

SSP Supply-Side Platform.

UI User Interface.

VPN Virtual Private Network.

Chapter 1

Introduction

As of 2021, there were more than 5 billion Internet users globally [Min21], and Internet-related services influence more and more people's daily lives. Social Networking Sites (SNSs) have become a large part of people's social interactions, giving the possibility of direct messaging and sharing photos, news stories, and political opinions. Smartphones allow people to stay up to date with everything going on anywhere in the world. Most online services are free, but they still come at a price, namely data, which has become a large part of the Internet economy. With information on every Internet user, it is possible to make accurate advertisements for a large portion of the world's population. In 2020, the online advertising ecosystem had a revenue of \$136.3 billion according to a report by PwC in 2021 [PI21]. It is essential to have a critical perspective on information collection in this ecosystem. What control do the users of these services have over what information they share, who they share it with, and for what it is used, and how do their attitudes surrounding privacy influence their decisions?

Furthermore, with the rapid growth and evolution of online services, it can feel difficult for a consumer to stay up to date with the latest developments. The development and improvement of data collection, data mining and Artificial Intelligence (AI) has made it possible for companies to categorize Internet users even more fine-grained to tailor features and advertisements directly to the relevant consumers. Although many may find this to be a feature that helps them navigate an abundance of online advertisements to find suitable products, others might feel like they have lost control over their information. There is a lot of money to be made from being able to predict the behavior and interests of, potentially, 5 billion people [ST17; BCW21; PI21]. With access to this kind of information, the holders of this data can perfect their services to match the wants and needs of the users, making it difficult for competitors to provide a good enough service to compete with the prominent actors [Zub19]. Additionally, selling this information to advertisers can also provide a generous income stream. Google, which has the largest tracking network online [KMBP18],

2 1. INTRODUCTION

has made a lot of money on advertising. In 2021, 80 % of Google's income came from advertising revenues, at \$206 billion [GE21]. Overall, there is reason to believe the saying "Data is the new oil" has some merit.

In this context, it is reasonable to have a critical perspective on who has access to this information and what value they place on it. As the key market players are private companies mainly focused on increasing their revenue stream, they have no inherent obligation to make user welfare and privacy their main priority. Similarly, in order to gain as accurate predictions as possible on as many people as possible, these service providers need people to use their services. Therefore, many services want to make it harder for users to exit their services by using mechanisms such as "endless scrolling" or "auto-play" [Zub19]. One other method to increase their user base is by acquiring smaller, popular sites for large sums of money. For instance, Facebook (now known as Meta) bought the popular photo-sharing app Instagram in 2012 and the popular messaging app Whatsapp in 2014 [BCW21]. In order to assure market dominance, Google pays Apple large sums every year to be the default search engine on iOS devices to secure its market dominance [BCW21]. These information networks extend the services themselves by inserting third-party cookies on websites that allow them to track users across large parts of the Internet. Thus, it is difficult to break free from the data collection web across different services. This constant information gathering makes it possible to create an accurate profile on a user based on all the sites visited, clicks, and searches made. Additionally, Facebook has been known to offer free Internet connections (on their sites) in developing countries to expand its user base [SAP+17]. Given this context, it can feel like people's lives are greatly influenced by decisions made by a handful of people in Silicon Valley.

There are some issues related to the use of data tracking and targeted content. Many may see the information collection of this scale to be a necessity of the free services of the Internet. However, it is concerning to see data leaks happening every year, causing sensitive information about people to be available for adversaries anywhere. It also is not easy to know how the data collected is used. For instance, the 2018 Cambridge Analytica Scandal revealed that information collected through Facebook was used for targeted political advertisements which could have swayed the 2016 US presidential election [CG18]. Additionally, the use of targeting can cause disadvantages for the consumer with price discrimination, blackmail and identity theft being some of the issues which can affect the lives of people [ATW16].

Some may hope for the prominent actors to regulate themselves. Developments recently suggest that Apple wanted to take measurements to improve its privacy practices. Their iOS 14.5 update introduced the possibility of asking not to be tracked between apps. However, some have criticized this by claiming it gives the user a false sense of security, as there is no legal obligation for the apps to comply with this

decision, as is the case with other "Do Not Track" requests [LH21]. Additionally, there can be issues given companies' significant influence, as they may leverage lawmakers to provide them with the freedom they desire. At the beginning of 2022, Mark Zuckerberg threatened to shut down Facebook and Instagram in Europe if they were not allowed to store their user data in the US [Gle22]. Since this is direct contrast to the rules of the [Eur16], such a misuse of marked dominance shows that the prominent actors are not afraid to use their power to change laws to their advantage.

Given this context, there has been a lot of focus on privacy in the last couple of years, . However, in many respects, there is little consumers can do to stop the information collection from taking place. Because of the rapid growth of online services, lawmakers have struggled to keep up with the emerging issues. While a detailed overview of how the key market players have gained their dominant role goes beyond the scope of this master thesis, it is clear that such events have allowed the web giants to gain their position. In later years there have been some attempts to introduce laws to give more power to the consumers. Most notable are the General Data Protection Regulation (GDPR) in the EU and EEA and the California Consumer Privacy Act (CCPA) in California, USA. However, years after GDPR went into effect, data tracking skyrockets [UTD+20], suggesting it has not had a great impact on information collection.

Previous research in this context has focused on user behavior and thoughts related to privacy management. In particular, research has been done on what makes users share personal information, and what price they place on their data. Additionally, users have been surveyed on the influence of privacy fatigue and privacy concerns have on privacy management. In user experiments, researchers have looked at how User Interface (UI) influences privacy behavior and how targeted advertisements compare to non-targeted advertisements regarding efficiency. However it is still unclear how privacy attitudes influence efficiency in privacy management. This thesis aims to gain more insight into what makes users struggle with managing their privacy and measures that could make the process easier.

1.1 Research Questions

Given this context, this thesis wants to contribute to better understanding the user perspective and still prevailing barriers in managing online privacy. The focus is on people's experiences with privacy, thoughts about targeted advertising and privacy management. The goal is to get an understanding of what consumers can and cannot do, and what hurdles are in place for people to achieve the privacy levels they desire. Thus, the research questions below will be the focus of this thesis.

***RQ 1:** What relationship do users have to their online privacy and privacy management?*

Hypothesis (RQ1): I hypothesize that most users do not think much about privacy in their daily life. Much of this, I believe, stems from the fact that the consequences of data collection is difficult to notice as well as being an ingrained part of every day life.

***RQ 2:** Which strategies do users use to control how their personal data is shared and used?*

Hypothesis (RQ2): I hypothesize that most users do not have many conscious strategies related to privacy management, and I suspect much of privacy settings are left on their default settings.

***RQ 3:** To what extent do users perceive privacy settings of different services as manageable?*

Hypothesis (RQ3): I hypothesize that most people find it challenging to find and manage their privacy settings. Additionally, I believe that there is a discrepancy in how well this perception matches how they in reality do.

These research questions are addressed using a mixed method approach. First, an online survey was conducted in order to get general data from a larger population. This study mainly focused on RQ1 and RQ2. Second, a user experiment focusing on managing privacy settings was conducted, focusing on RQ3. Combined with this user experiment, an interview was conducted in order to get insight into how the user experiment was and to gain greater understanding of the data collected in the online survey. This made it possible to get a better understanding of what issues people experience in their privacy management. The contribution of this thesis is to shed light on how privacy attitudes influence privacy management. Additionally, it shows how implemented barriers might hinder users from making proactive choices regarding their privacy, and what might help make privacy management more accessible.

This thesis has seven main chapters: Introduction, Background, Related Work, Methodology, Results, Discussion, and Conclusion and Future Work. The introduction chapter gives motivation for the thesis and introduces central research questions. The background chapter explains the theory behind targeted advertising and information collection and its value and relevance. Additionally, it focuses on some psychological aspects that might influence privacy management. After that, the chapter on related work summarizes some previous studies and their findings. In Methodology, all of the methods used for collecting data are explained, with a detailed explanation of the setup. In Results, the findings from the studies are shown, while Discussion debates the results and how it fits into the theory. Conclusion and Future Work sums up the thesis and suggests how future studies might build on the results.

Chapter 2

Background

Targeted advertising is "*advertising methods that deliver individually catered advertisements based upon the web site's content, location of the user, browsing history, demographics, the user profile, or any other available information*" [FB12]. This type of advertising is designed to make it more likely for the advertisements to reach the individuals who would be most interested in the given product. Section 2.1 of this chapter focuses on the inner workings and motivation for using targeted advertising, while Section 2.2 focuses on the human factors influencing privacy management. Lastly, Section 2.3 focuses on the General Data Protection Regulation (GDPR) and how it has influenced data collection. This chapter sketches the broader context in which the related work (Chapter 3) and the research presented in this thesis should be situated.

2.1 Behind Data Collection and Targeted Advertising

In order to understand *why* the use of data collection is prevalent on the Internet, it is interesting to see how it works and the motivation for gathering data to the extent that is collected today. This section discusses the details behind data collection and targeted advertising as well as the value of collecting information for this purpose.

2.1.1 How Does Targeted Advertising Work?

For there to be accurate, targeted advertisements, a few elements have to be in place. First, there must be a way to identify and categorize which users are relevant to the advertisers. Additionally, there has to be a way to collect information on users such that they are shown advertisements relevant to their interests. According to Zuboff, in her book "*The Age of Surveillance Capitalism*", the Big Tech companies sell "prediction products" on their users [Zub19]. The goal is for them to know as much as possible about their users in order to predict their future behavior. If a user, for instance, has searched for a restaurant in their area, Google can sell this information to interested parties. By doing this, restaurants can, for instance,

advertise directly to the people interested in finding somewhere to eat at this moment, based on location and time.

Users are assigned unique identifiers to make personal profiles for advertising. Whenever someone is using a website, they leave some information behind. While users might give some information knowingly, websites or apps might collect other types of metadata without the user's awareness. The website gathers this information to customize the user experience or train the system algorithm to improve its services [Zub19]. However, this information can also create an accurate picture of the person themselves. There are three types of personal data, as depicted by Birch et al. [BCW21]; identifiable, anonymous and pseudonymous data. Identifiable data is given knowingly and voluntarily while anonymous data is the opposite, and often gathered through data processors. Pseudonymous data is gathered through third parties. Despite these distinctions, evidence suggest that all of these types of personal data can be used to identify a person [Edw18]. Through an advertising network, information can be gathered from many different sources, merged, and used to create interest profiles. Such interest profiles are made based on the users' demographic and psychographic traits and their behavioral data [DN18]. These profiles can help predict what type of advertisements a user is most likely to respond to and are used to display relevant advertisements to the right people.

The most common way to store digital identifiers is through HTTP cookies. Cookies can save states in the otherwise stateless HTTP protocol [Kri01]. A common use for cookies can be a shopping cart that remembers selected items during online shopping. Additionally, cookies allow users to stay logged into a site every time they refresh, improving the user experience. However, this is also a way for online advertisers to get insight into the habits of end-users. The cookies can store a unique identifier on a user for the server to recognize the individual in subsequent sessions [UTD+20]. A *first-party cookie* is set by the website a person visits, while another domain sets a third-party cookie with an object inserted into the original website [UTD+20]. From this, online advertisers could get insight into the users' interests or geolocation, which is valuable for displaying the correct advertisements when the website loads on the browser. Although the Same Origin Policy states that third parties might not share their cookies directly, this is bypassed by using *cookie syncing* [UTD+20]. Cookie syncing allows third parties to share user identifiers with other third parties [EN16]. Because of this, the web of information on users is quite extensive. Englehardt et al. found that any two of the top 50 third parties participating in cookie syncing have an 85% chance of having at least one cookie in common [EN16].

Another way to identify users is through the use of *device fingerprinting* [NKJ+13]. While cookies can be deleted by users, either when closing a session or deliberately,

device fingerprints are stored on the server-side. Additionally, users might implement browser extensions that limit the use of third-party cookies. This unavailability of cookies is one of the reasons why there was a desire to find different ways to track users [NKJ+13]. Device fingerprinting relies on metadata from the user, such as which operating system they use, their IP address, the language they have set, battery percentage, etc. to identify a person with relative accuracy. However, many have criticized device fingerprinting as privacy intrusive since there is no real way for users to opt out of this practice [NKJ+13]. Although a user might use a "Do not track" signal, which tells the website that they do not wish to be tracked, there is no actual obligation for them to comply [TSLB21].

The ecosystem of targeted advertising mainly consists of three primary entities [UTD+20; LC20; DN18]. A Supply-Side Platform (SSP) is used by publishers to sell their available advertising space to interested parties. This could, for instance, be an online newspaper. On the other side, there is a Demand-Side Platform (DSP). The DSP helps an advertising company automate their advertising campaign by directing the advertisement to the relevant users. This is done with the help of a Data Management Platform (DMP), whose main task is to gather and process the information on users. The DSP requests an audience with specific characteristics, and the DMP provides a list of relevant users to match the request. The SSP provides users who are available through the publishers' platforms. If the users provided from the SSP match any of the users found by the DMP, the DSP will participate in the auction for this advertising space. This form of advertising is managed through *programmatic buying*, which means that the process of buying advertising space happens automatically through Real-Time Bidding (RTB) in an ad exchange [LC20]. The DSP is responsible for purchasing the advertising space for their clients at the lowest possible price, while the SSP is responsible for selling the advertising space of their clients at the highest possible price. These auctions happen every time a browser loads a website [UTD+20]. Rather than buying the advertising space in itself, this form of advertising aims at buying the desired *audience* [LC20]. A person with the browser extension "Adblock", which filter out advertising on web pages, will not be measurable or legible as a "user" in this system [BCW21]. Figure 2.1 depicts a simplified version of this process.

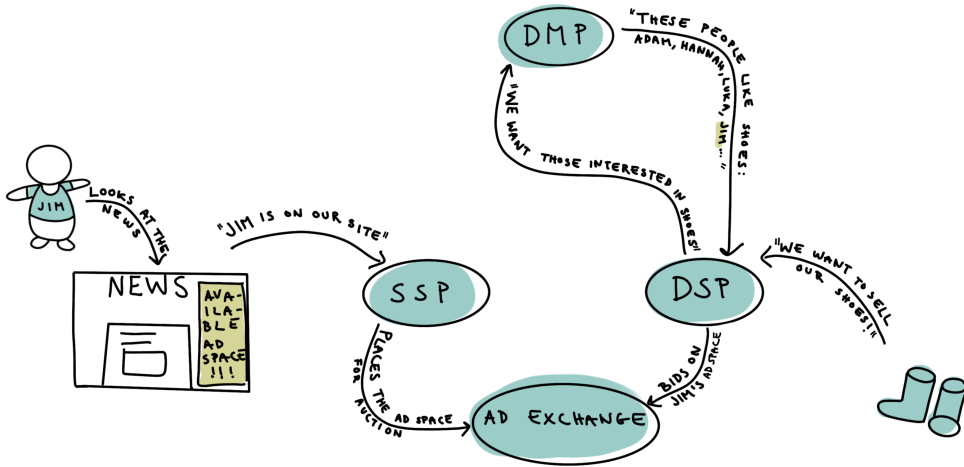


Figure 2.1: A simplified explanation of how advertising spaces are bought and sold.

2.1.2 What Is Targeted Advertising Worth?

As previously mentioned, targeted advertising allows companies to advertise directly to the consumers who are most likely to respond positively to their campaigns. This form of advertising is more effective than traditional advertising. An article from 2012 found that targeted advertising was nine times more likely to generate brand searches and 4.5 times more likely to click on a targeted advertising over a non-targeted advertising [FB12]. Tucker found in her article, *Social Networks, Personalized Advertising, and Privacy Controls* that targeted advertisements on Facebook were at least twice as effective as non-targeted advertising [Tuc14]. This article is discussed in depth in Section 3.2.4.

Given this context, it is fair to assume that there is an incentive to gather user information to increase advertisement revenue. In its annual report from 2021, Alphabet reported that about 80% of its revenue came from advertising [Alp22], which constituted a total of \$206 billion from advertising. In turn, Meta reported in their annual report a total advertising revenue of \$115 billion, which was about 97% of their total revenue this year [Met22]. Using targeted advertising, companies can auction the user’s information to advertisers with relevant products. In iOS 14.5, Apple made it possible for users to disallow tracking between apps. The users were given an active choice the users had to make for every app they used. According to Gizmodo, about 96% of Americans did not allow tracking between apps when given a choice [Sta21]. This change made it so that the apps could not send the ID of the users to advertisers if they did not consent. The change caused app companies

such as Meta and Snap to experience a fall in their advertising revenues and a fall in stock prices [Sta21; Les22]. In 2022, Facebook estimated a \$10 billion loss due to this change [Les22]. Although this privacy feature has been criticized for giving users a false sense of security [FH21], it shows how much information collection matters for advertising revenues.

The exact value Big Tech places on personal information is not easy to estimate, as stated by Birch et al. in *Data as an asset? The measurement, governance, and valuation of digital personal data by Big Tech* [BCW21]. In many ways, the companies are incentivized to have the users' attention for as much of the time as possible, as a means to gather information and have available advertising space for the user in question, thus playing into the attention economy. This is done by using mechanisms such as *auto-play* and *constant scrolling* to make it more difficult to exit the platform in question [Zub19]. Another way to ensure user attention is to eliminate competition by acquisitions. One of the ways in which one can assess this value is by the extent to which companies acquire smaller successful platforms. One example of this can be seen when comparing the differences between Big Tech with other Top 200 companies. Between 2010 and 2019, Big Tech spent an average of \$23 billion on acquisitions [BCW21], while the average sum was \$8.4 billion for the Top 200 companies. By monopolizing the users and engagement, the companies increase their market value. In 2020, The House of Representatives released a report stating that Facebook "*selectively enforced its platform policies based on whether it perceived other companies as competitive threats. In doing so, it advantaged its services while weakening other firms*" [NC20].

2.2 The User Perspective of Privacy Management

When now turning to the perspective of how users deal with such targeted advertising mechanisms and practices, Acquisti et al. stated in their article from 2020 that "*privacy is extraordinarily difficult to manage or regulate in the Internet age*" [ALB20], even though most people are interested in protecting their personal space, both physically and online [ALB20]. While a study from 2013 by Rainie et al. found that 86% of users had taken measures to hide their digital footprints, they also found that 59% also believed that it was impossible to be completely anonymous online. The feeling of lack of control may stem from both psychological (Section 2.2.1) and implemented barriers from the sites themselves.

2.2.1 The Psychology of Users

Human psychology is a part of the explanation to why online privacy management can be challenging. These aspects may influence the ability of the users to make well-informed decisions regarding their privacy while also making it difficult to take

active measures to achieve the level of privacy they ideally would prefer. This section will explore the influence of different psychological concepts that affect user behavior and are sometimes used by online companies to gather information on their users. Most of these concepts are taken from the 2020 article, *Secrets and lies: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age* [ALB20].

For many users, it can be challenging to make well-informed decisions regarding their privacy. *Information asymmetry* refers to the discrepancy between what the users know about how their data is collected and how it actually works [ALB20]. This lack of accurate information causes the users to be unable to make an informed decision regarding their privacy and makes them less likely to respond to the risks. This inaction allows firms to increase their data collection and usage. In this regard, the concept of *bounded rationality* refers to the lack of capacity by consumers to process and makes sense of the information they are presented [ALB20]. This is evident in the reading of privacy policies, where many reports do not read them before accepting them. Obar and Oeldorf-Hirsch found that 73% of the participants in their study skipped the privacy policy entirely, and of those who did read the policy (~ 8000 words), the median time spent doing so was 13.6 seconds [OO20]. Often, companies will write long and difficultly worded policies, using legal terms most users will not understand [ALB20]. Additionally, the constant request for consent may result in *consent fatigue* for many users [RTKvE18]. This results in the users being overwhelmed by the continuous need to make privacy choices and feeling like they can not read through and understand all of the options they consent to.

Another factor influencing privacy management is the ability to see the importance of privacy protection. Humans, in general, are prone to *present bias*, meaning that users are more likely to respond to costs and benefits that are immediately noticeable [ALB20]. The ramifications of privacy management is notoriously difficult to see. Thus, minor inconveniences, such as extra time and effort, are often enough to stop people from making better privacy decisions. An example of this is with cookie requests, where the sites often give the users an option of "accept all" or "manage option", the latter requiring a few extra clicks which might be enough to stop people from making an active choice. People are also bad at assessing negative consequences with small probabilities. The immediate benefits of sharing their data are direct and tangible for many users, while the consequences are *intangible* and difficult to quantify [ALB20]. Additionally, people might feel like they are not in control of their information, causing a sense of weariness towards privacy issues. This is referred to as *privacy fatigue*, in which the individuals believe their actions have no effect on their privacy management [CPJ18].

There are several additional psychological factors which might cause poor privacy choices. *Constructed preference* refers to the users being uncertain of their preferences,

making them more likely to maintain default settings on the sites they use. The firms may exploit this by setting these to be advantageous to increased data collection rather than protect their users' privacy. Additionally, and perhaps counter intuitively, the sites might give their users more granular control over their privacy management, causing them to share more information and be less critical of what they share. This concept is referred to as *illusory control* [ALB20]. One example of this is further discussed in Section 3.2.4, where Facebook users were far more willing to click on targeted and personalized advertisements after being given more granular control of their privacy [Tuc14].

Another aspect is that it is easy and enjoyable to share personal information on the Internet. Firstly, people are influenced by each other. When users see other people share on SNSs, they are more inclined to do so themselves. This concept is referred to as *herding* [ALB20]. Sites may exploit this by making it seem like "everyone" else is sharing what they do online, making it more appealing for others to do the same. Additionally, people like to share what they are doing and have a *drive to share* [ALB20]. Lastly, people are good at *adapting* to constant or gradual increases of risks. This may be exploited by companies gradually increasing their data collection and changing their data use practices [ALB20].

2.2.2 False Sense of Security

Some users will experience a *false sense of security* due to some of the privacy-related choices. In a study from 2014, Hoofnagle and Urban found that many Americans believe privacy policies are meant to protect their privacy, although this is not the case [Hoofnagle2014ALANECOMICUS]. Additionally, some are given options that may seem like they give them better privacy protection, even though it may not work as intended. One such example is the use of "Do Not Track" signals, in which browsers give the option to users to indicate to the pages they visit that they do not wish to be tracked [TSLB21]. However, there is no requirement for the sites to abide by the users' wishes. In April of 2021, Apple released an update for iOS 14.5, which would give the users an option of allowing or disallowing tracking between apps. In doing this, the apps would no longer be allowed to share the user's ID for advertising purposes [FH21]. However, a study made by ex-Apple engineers five months after this update found no difference in the total amount of third-party trackers [LH21]. Instead of the ID itself, the apps that use metadata to use device fingerprinting, as discussed in Section 2.1. The issue with this false sense of security is that users believe they are protected when they are not. Additionally, it plays into the *Illusory control* mentioned in Section 2.2.1, as users are more likely to be less critical of the data they are giving away if given more granular control over their data [ALB20].

2.2.3 The Privacy Paradox

The term *privacy paradox* was first coined by Susan Barnes in 2006 when she discussed the amount of information teenagers were willing to share online, while their adult counterparts were concerned with invasion of privacy [Bar06]. Today, the term refers to the phenomenon where people say they are concerned about their privacy while simultaneously partaking in privacy-compromising behavior [BdJ17]. Research has shown that most people are willing to share personal information for small rewards. One such study, discussed in Section 3.2.3, showed that 88% were unwilling to sell their data when asked, but when people were given €5 for filling out a form with personal information (unaware that the study measured them on privacy attitudes), 83.3% complied [BN18]. This shows that the reported levels of privacy concern people report, might not match their overall approach to privacy management. However, research has also shown that privacy concern does affect privacy attitude and behavior [DT15].

2.2.4 Achieving Desired Levels of Privacy

When considering these implemented and psychological constraints, is it feasible to reach the level of privacy one wishes for? Although there are tools available to reach higher levels of privacy, Acquisti et al. [ALB20] argue that *"the increasing value of monetizing personal data increases firms' demand for tracking, thus driving down the supply of privacy"*. Due to network effects, a lack of competition, and strong lock-ins, the options users have are limited [ØA21], since much of the value of services lies in the users of the services. Most notably, services based around people, such as SNSs and instant messaging services, are dependent on having as many people as possible on their sites to have value to the users. This causes strong network effects and makes the cost of using more privacy-conscious services much higher for privacy-focused users. Additionally, the use of services can train the performance of a system to make the product as good as possible. For instance, Google's search engine can make accurate predictions about what a user is searching for due to its massive user base and well-trained algorithm, which gives them a considerable competitive advantage [Zub19]. On the one hand, this provides the user with a more valuable product, but on the other hand, it eliminates competition, giving the users fewer options [ALB20].

2.2.5 The Importance of Privacy Management

For the user, there is a cost of protecting privacy, as well as a cost of not doing so. On the one hand, the use of personal data makes it possible to have more enjoyable content specifically catered to the wants and needs of the individual. Additionally, it is advantageous for the advertising industry, as they can more accurately reach their desired audience with a campaign. However, the problem is that *"there is no practical way for consumers to regulate the use of their information meaningfully"*

[ALB20]. The incentives to collect information are so strong that the marginal cost of data protection increases dramatically with higher privacy protection.

There are instances in which the information gathered about an individual may even hurt them in some way. For one, users may experience *price discrimination*, a concept in which a company may leverage information on previous behavior to give the individual a higher price for a product than they otherwise would [ATW16]. This could, for instance, be an airline who gives higher prices after a person searched for tickets previously or a product that has a higher price to different people due to shopping habits. For instance, Tinder was criticized earlier this year for having significant discrepancies in pricing for their premium subscriptions depending on the user [Hor22], with age being one of the factors they found to give higher prices. Another issue with the focus on data collection for targeted advertising is their part in the attention economy, as previously mentioned. Additionally, there is always a risk of data leaks, that might result in sensitive information being in the hands of adversaries. Other examples may include identity theft, blackmail, and social stigma [ATW16].

A more extreme example of the consequences of such data collection systems is The Cambridge Analytica Scandal. In 2018, the British newspaper The Guardian revealed how the 2016 US presidential election and the referendum determining whether or not Britain should remain in the European Union were influenced by political targeted advertising [CG18]. Cambridge Analytica was a company specializing in the strategic use of data mining and analysis. In 2014, hundreds of thousands of users were paid to take a personality test through an app, which they consented to be used for academic purposes. However, this information was then combined with data from the participants' Facebook friends, creating a large pool of information [CG18]. Led by Donald Trump's key advisor Steve Bannon, the company built a system that could target and profile potential voters in the US. This information was fed into the Facebook advertisement system and targeted small groups of voters who had the potential to swing the election [Dat20]. Not only did these campaigns try to target potential voters for the Republican Party, but they also targeted groups of potential voters for the Democratic Party to abstain from voting. This scandal showed how much influence targeted advertising can have on society.

2.2.6 What Can be Done to Change the Privacy Imbalance?

There are three main categories of options to improve privacy for users. First, there is the option to use individual solutions. This is done with the help of Privacy Enhancing Technologies (PETs), which could entail using a Virtual Private Network (VPN) or onion routing to hide personal information [AAB+17]. However, the issue with this approach alone is that it requires the user to stay on top of the situation to

adjust according to changes that may occur. Additionally, there may be a barrier to using such services if the user does not know how it works or is unwilling to pay for them. The second way of increasing privacy is through *interface solutions* [AAB+17]. This could, for instance, mean providing the users with more transparency about their choices or having less lenient default privacy settings. The iOS update Apple made with tracking, mentioned in Section 2.1.2 and 2.2.2, is an example of such a solution. However, the issue with this approach is that all the power lies with the companies in charge of the interface, who might not have incentive to prioritize the users' privacy. Lastly, there are *regulatory solutions*. These are government-issued regulations that the companies must follow in the given region [AAB+17]. One example of this is the GDPR, discussed more in Section 2.3, which all companies who have Internet users in the European Union have to follow if they do not wish to be fined. The issue with this approach is that such legal proceedings require a lot of time, as well as it being challenging to keep up to date with quickly changing threats. Additionally, there might be issues with *regulatory capture*, in which the regulatory state agencies are manipulated by the industries they are supposed to be controlling [Dal06].

2.3 General Data Protection Regulation

In May 2018, the arguably most prominent and influential government-issued regulation thus far was taken into effect in Europe, the GDPR [Eur16]. This regulation aimed to give the data subjects give personal data better protection, increase transparency, and give stronger intervention rights to the data subjects [MHF19]. Many of the points central to the GDPR tackle some of the issues discussed in Section 2.2.1, especially regarding *information asymmetry*, *bounded rationality*, and *constructed preference*.

The GDPR has some key points central to the collection of data and privacy management. For one, the GDPR requires all companies processing data on European citizens to be "*processed lawfully, fairly and in a transparent manner*" [Eur16]. This implies that the data processing should have a legitimate purpose and only take place for the stated purpose. Additionally, the companies have to inform the data subjects regarding the processing of their data [Bha18]. Another key point in the regulation is the "*limitation of purpose, data, and storage*". Companies should limit data collection and processing to only include what is strictly necessary, known as the "*data minimization principle*" [Eur16], and delete personal data once the processing is completed [Eur16; Bha18]. If a company wishes to collect and process data beyond legitimate purposes, they need consent from the data subject, who is allowed to withdraw their consent at any time. For there to be lawful processing of personal information, consent has to be "*given freely, specific, informed and unambiguous*" [Eur16]. Lastly, companies should incorporate privacy by design [Eur16; Bha18].

Two main objectives of the GDPR are to; (1) protect "*natural persons with regard to the processing of personal data [...]*", and (2) protect the personal data of natural persons [Eur16]. In the context of targeted advertising, the GDPR should have impacted the data collection and processing to some degree, as it should have made it more difficult to collect information without specific and legitimate purpose.

2.3.1 Changes in Privacy After the GDPR

What differences can be found in the advertising networks after the GDPR was taken into effect? As described in Section 2.1, the advertising ecosystem uses HTTP cookies to collect information and identify users online and cookie syncing to share information within a network of third parties. With the GDPR this process experienced some changes due to the limitation of data collection. Urban et al. studied the impact of GDPR in the advertising networks using graph analysis and studying cookie syncing on a browser level [UTD+20]. They found a "*steep decrease in [cookie] sharing after the GDPR went into effect*" [UTD+20], implying that while fewer actors may have been allowed to do so, collect the data. Additionally, they found that "*the average number of third parties embedded in websites did not change*" [UTD+20], suggesting that the new regulation did not affect the amount of data collected and processed. While they did not find noticeable differences in the advertising ecosystem, they did notice a switch from smaller networks to larger ones, such as Facebook or Google might provide. Overall this might have had a harmful effect on user privacy as "*fewer companies continue to be present on more websites, increasing their possibilities to create profiles*". This change might have occurred because the increased legal consequences might have made it more difficult for smaller actors to compete with the larger actors, causing the larger actors to increase their market shares [GB21].

Momen et al. did a study exploring app privacy changes before and after GDPR [MHF19]. This study focused on the use of the *dangerous permissions* on Android smartphones. Previous studies had shown that apps requested more permissions than they needed for the purpose of the app, which became the basis of the study as the GDPR focuses on limiting data collection to what is strictly necessary [Eur16]. Their study found an overall decrease in the number of permission requests; however, the requests for sensor-related permissions had become greedier. These types of settings include access to camera and microphone, as well as body sensor-related access [MHF19]. One of the reasons this might be, they speculated, for the purposes of targeted advertising. By having access to such settings, they can advertise to the user while they are looking at their screen. There also seemed to be an increased request for GPS location, suggesting an increased interest in location-based advertising. Interestingly, they also found many apps had many unused permissions [MHF19]. Overall it seemed like the new regulation had not changed the number of used permissions, but rather changed "*the ways in which permission consent is obtained*

from the app users" [MHF19].

Overall, the introduction of GDPR appears to have changed how companies have to process personal data, focusing on transparency and consent and increasing the protection of users. However, it has not necessarily reduced data collection but instead changed how information is shared and used. It seems like one of the most significant differences is with the number of actors decreasing, while the size of the actors is increasing.

Chapter 3

Related work

There have been several studies done related to the objectives of this thesis. Many large-scale studies have been conducted to understand what influences users regarding privacy management. These studies are often suitable for getting a general opinion from a population but might not give accurate answers in hypothetical scenarios. In addition, some privacy user experiments have been conducted to find what users do in a controlled, non-hypothetical environment with concrete and realistic tasks, providing a better picture of how the participants would respond in real situations. This section includes a summary of some key studies relevant to the rest of the thesis.

3.1 Large Scale Surveys

A first set of studies are based on larger-scale and cross-sectional study designs.

3.1.1 What Makes Users Share their Information with Advertisers?

In a 2013 study, Leon et al. explored the factors that affected users' willingness to share information with online advertisers [LUW+13]. Their online survey had 2,912 participants assess different privacy policies on websites and evaluate their willingness to share information. They changed different dimensions to determine which elements would make the most impact. Firstly, users were given different scopes of use, meaning who would collect the information and what it would be used for. Second, there were different data retention periods, either one day or indefinitely. Finally, some were allowed to edit and delete the information collected, while others had no such control mechanisms. In addition to this, they had one real website most would be familiar with (WebMD) and a fake website they made up themselves to assess whether the familiarity of a site impacted the trust of data collection.

The study found that the most important factors were the scope of use and data retention period. They also found that familiarity with the website and granular

control over data collection did not impact the willingness to share data. In addition, they found that although half of the participants were unwilling to allow any data collection, most participants were not willing to pay to prevent data collection. It is worth noting that this study was done in 2013, possibly giving different results than it would today. In particular, there has been an increased focus on privacy and data collection in the past years, which might have resulted in different results today. However, this study still has some interesting findings on data collection for the purpose of targeted advertising which might still be relevant.

3.1.2 What Affects Users Attitudes Towards Privacy Policies?

A 2021 study by Ibda et al. explored the attitudes affecting user perceptions of privacy policies [ILRB21]. In this online survey, 655 participants were asked to explain their behavior towards privacy policies and what motivates them to read or ignore them. Additionally, they were asked about their attitudes towards opt-out services. They were then given excerpts from different privacy policies and asked to assess the readability and whether they were willing to turn down a service with an invasive privacy policy. They were also presented with different privacy policies of websites to assess their user-friendliness. The study found that most participants occasionally try to read privacy policies, although most of these people had never completed reading a privacy policy. In addition, 22.5% of the participants in the study had never attempted to read a privacy policy. When given an excerpt of a privacy policy, only 18.4% thought it was difficult to understand, while 55% of the participants answered incorrectly when asked to interpret its meaning. This shows a significant handicap with the overall comprehension of the policies. The study participants were asked whether, based on excerpts, they thought the information collection made by Google, Amazon, and Facebook was concerning or unjustified. They found concerns with the policies with 44.4% of the participants for Google, 53.3% for Amazon, 55.1% for Facebook's information collection, and 59.9% for Facebook's collection of signal data from Bluetooth, WiFi, and mobile phone towers. This last point was found unjustified by 79.9% of the participants. Additionally, they found a significant correlation between how user-friendly the interfaces for reading the policies and their willingness to read the privacy policy. Over 75% stated that they felt pessimistic about the design of privacy policies, listing this as a significant reason for apathy towards reading them.

A limitation of this study lay in the participants of the study. All of the respondents are American, meaning they are subject to different privacy regulations than we are in Europe. In addition, the researchers recruited the respondents through Amazon Mechanical Turk, which might affect the legitimacy of the responses as the respondents are paid for the number of surveys they complete.

3.1.3 How do Users Interpret Technical Terms in Privacy Policies?

A 2021 study was conducted about the interpretation users had of technical terms in privacy policies [TSLB21]. Tang et al. wanted to "*evaluate how well users understand technical terms that appear in privacy policies*". First, they did a pilot study, where they had the participants explain technical terms in their own words. Based on this, they selected 20 terms that were commonly misunderstood to include in the main study with multiple-choice questions and two terms that were generally well understood. Additionally, they tested how comfortable users were with technical terms and privacy policies, where they replaced the technical terms with descriptive language for the same terms. The final study had 1159 participants, of which 800 were analyzed after passing tests for giving reliable answers.

The results of the study revealed that many of the technical terms used in privacy policies are misinterpreted. Furthermore, the term *privacy policy* was misinterpreted by 71% of the respondents, who believed that a privacy policy guaranteed "data protection, confidentiality or consent". There was a significant difference in comfort levels between the technical and non-technical policies. Technical terms related to tracking especially decreased comfort levels, while other terms such as *browser storage* and *local storage* gave increased comfort when explained in a non-technical manner. Additionally, the study surveyed the likelihood of accepting a policy and found that this was slightly higher than their comfort level, confirming the assumption that users are willing to accept privacy policies that they might not feel comfortable with. The study also looked at how having a technical background affected the answers. The most significant differences lay in the *I don't know* category, where only 4% of the technical participants chose this option, compared to 14.77% of the respondents without a technical background. Interestingly, the difference in correct answers, was not as significant, with technical participants answering 41.97% correctly against 38.49%. Overall, the study concluded that "*the use of technical terms in privacy policies is a barrier to informed consent*."

This study also used Amazon Mechanical Turk to recruit its participants. Their percentage of correct answers is quite low, which might be because they predominantly used the misunderstood terms from their pilot study, and might therefore not give a complete picture of the participants' knowledge.

3.1.4 What Role Does Privacy Fatigue Play in Privacy Management?

Choi et al. studied privacy fatigue's role in online privacy behavior [CPJ18]. They claim that privacy fatigue has two dimensions - emotional exhaustion and cynicism, which impact how people respond to making decisions. Their study surveyed the over-

all privacy concern among the participants and their privacy fatigue, disengagement, and their intention to disclose personal information. They hypothesized that greater privacy concerns would result in less intention to disclose personal information as well as less disengagement. Additionally, they hypothesized that the opposite would be true for people with high levels of privacy fatigue. The study results supported their hypotheses, specifically a high level of privacy fatigue being a strong predictor of disengagement among all users regardless of their demographic characteristics. They also found that *"privacy fatigue has a stronger influence on the behavior of users than their privacy concern"*. This might be a contributing factor to why privacy concerns might not always predict privacy behavior accurately.

All of the respondents in this study are from South Korea. As in the American study, this might give a different result than Europe because of regulatory and cultural differences.

3.1.5 How do Privacy Concerns and Self-Efficacy Influence Privacy Management?

A study by Chen and Chen from 2015 investigated how privacy protection in SNSs are influenced by privacy concern and efficacy in privacy management [CC15]. The study recruited college students in their first year in the US and was focused on Facebook as an SNS. 559 students answered the study, and 515 of the responses were used after removing invalid answers. They found that privacy concerns were positively related to limiting profile visibility and *fiending* other users. Self-efficacy in privacy management was positively correlated with limiting profile visibility, although not as much as the privacy concerned individuals. Interestingly, being self-efficient in privacy management was positively related to self-disclosure, meaning that the Facebook users with the most privacy management skills were also more likely to share information about themselves.

The survey of this study was conducted in 2011, which makes the data somewhat outdated considering the development of social networks in the last decade. Additionally, they only surveyed first-year college students, making it difficult to generalize the results to the broader population. Although this study focused on data sharing in general and not only on visibility settings, it still only focused on the privacy settings on Facebook. Results from other sites might yield different results.

3.1.6 Privacy Attitudes in Norway

The Norwegian Data Protection Agency (Datatilsynet) released a survey mapping the Norwegian public's attitude towards privacy and familiarity with the privacy regulations in 2020 [Dat20]. The survey had 1501 respondents and surveyed the respondents' knowledge of privacy regulations, how much control they felt over their

information, who they trust, their willingness to share personal data, and their attitudes towards targeted advertising. In general, the respondents were concerned about their privacy. Half of the polled individuals expressed that they had avoided using a service because of lacking trust in the business. 7 out of 10 felt like they had little control over how their personal data was stored and used on the Internet. 3 out of 4 were negative to personal data being gathered for targeted advertising purposes. The majority was negative about sharing their banking details, social security numbers, interpersonal communication, and biometric information.

This study was based solely on the answers participants gave related to privacy behavior, which might not necessarily comply with privacy behavior, as discussed in Section 2.2.3.

3.2 User Experiments

Reported behavior does not necessarily match how people actually behave. A second set of studies are based on research on how people behave in more realistic scenarios, rather than relying exclusively on their reported actions as it potentially has a bias. Thus, this set of studies is based on the experimental paradigm.

3.2.1 How Does the User Interface Affect Engagement with Privacy Features?

In order to investigate how to best make users engage with privacy features on SNSs, Namara et al. conducted an online user experiment studying the effects of different privacy adaption methods [NSK22]. In the study with 406 participants, a Facebook-like SNS platform ("FriendBook") was presented with a scenario in which they were a person looking for a job. The participants were given different tasks to moderate their profile to be more appealing to potential employers. There were three other adaptation methods that they tested. (1) Automation, where the privacy feature was automatically employed, with a notification where the participants had to reverse the decision if they actively disagreed. (2) Highlight, where the researchers highlighted the path to the privacy feature in yellow. (3) Suggestion, where a *suggestion box* would appear with a suggested privacy feature that they could accept. In addition, they had a control group with none of the features and groups that had some features tailored to their previous familiarity with them. Their study found that automation of all features gave 98% privacy protection, while suggestions gave 68% protection. Highlighted features (40%), gave no significant protection over the control group with no adaptations (39%). Their study also found that suggestions provided the most user engagement (68%), with suggestions giving the most perceived usefulness. Interestingly, they found that not automating all privacy features, which might be unwanted by users, resulted in higher privacy protection (99%).

This study also got their participants from Amazon Mechanical Turk, which can give some unreliable answers, as discussed in 3.1.2. This study was also limited to only American participants. Because the researchers did the study online without guidance, there is a possibility that they were not able to capture the thoughts that went into the different actions, seeing as there could be explanations as to why they did not apply the suggested privacy protection. Additionally, as this was a fictive scenario the participants might have interacted differently with the prototype than they would on their own profiles.

3.2.2 What Value do Customers Place on Their Personal Data?

A German study from 2018 used a field experiment in order to find the value people set on their personal data by asking customers at a bakery delivery service for consent to share their data with third parties [PW18]. A contact person from the service would call the clients in order to ask for their consent, which was incentivized by offering them a 5% discount off their purchases for the last three months. The study had 177 households, where 88 were only given the percentage of their discount, while 89 were given the exact amount in Euros. In their study, 30.5% consented to share the data, even though 52.3% were already participants in other bonus programs. The threshold for consent for this study seemed to be €5-€6. They found that a high enough offer made consent more likely when the price was not explicitly stated.

This study was conducted in Germany, making it more applicable to the general demographic in this master thesis, as they are also under European privacy regulations. However, even though the study is from 2018, the interviews were done in 2014, which was many years before the general population of Europe was familiar with the GDPR. Furthermore, the study participants were limited to the customers of one bakery delivery service in Germany, where only one person from each household talked to the contact person. The population of this study is somewhat limited as 73% of the participants were female, with a minimum age of 25 and a maximum age of 87. Additionally, the participants would have to be able to afford such a service, which might mean that they are less susceptible to the discounts offered to consent. Thus, the study might not accurately represent the region's general population.

3.2.3 How Willing Are Users to Sell their Personal Data?

Benndorf and Normann did a study in 2018 on the willingness to sell personal data in laboratory experiments [BN18]. The study was divided into three parts. First, they made the participants place the minimum value they would accept for different kinds of data. The researchers incentivized the 128 participants by paying them (€1-€50) if they suggested a price lower than a randomized draw. Second, they used a "Take it or leave it" (TIOLI) mechanism, where 108 participants of unrelated studies

were asked to fill out a form in order to receive an additional €5. Both of these studies had different kinds of information requested, namely anonymous preferences, contact information, and a combination of the two. Additionally, the first study had different kinds of Facebook information as well. Lastly, they had a large-scale telephone survey with 1000 participants to survey the general population's attitudes on privacy attitudes.

In both the first survey and the TIOLI survey, they found that five out of six participants were "willing to sell non-anonymous personal data for commercial usage". On average, the participants requested €15 for contact data and €19 for the information from their Facebook accounts. However, 83.3% of the participants of the TIOLI study were willing to share the non-anonymous information in exchange for €5, and 100% gave up the anonymized information. The results of the large-scale survey revealed that 88% of the population would be unwilling to give consent for sharing all data bundles. This result shows a significant discrepancy between what the users say they would do in a hypothetical scenario, and what they actually do.

Because the large-scale survey was done as a phone interview, which might give a bias regarding the sampling of who is on the calling list and who answers such a survey. 90% of the population of this large-scale survey was in the age range 18-29, which does not represent the German population. The explicit focus on privacy in the BDM survey and the large-scale survey might also have given more room for the participants to be privacy-aware than they usually would be.

3.2.4 How Does Targeted Advertising Compare to Non-Targeted Advertising?

In 2010 Tucker performed a field experiment using Facebook advertising for a non-profit organization [Tuc14]. The advertisements reached 1.2 million Facebook users over a span of five weeks and measured the click-through rate of the advertisements. The advertising campaign's goal was to increase the number of followers on the non-profit Facebook site. In the middle of the experiment, Facebook changed their privacy settings to be more transparent and manageable after public backlash. Thus, the experiment could study the effects this change had on the effectiveness of the advertising campaign. There were three different types of advertisements. There was a baseline non-targeted advertisement, a targeted but not personalized advertisement, and a targeted and personalized advertisement. The targeting factors were based on whether they followed one of 19 celebrities who had previously supported their cause, or if they had graduated from one of 20 colleges with a reputation for supporting their cause. The non-personalized campaign had general characteristics in their text, while the personalized named the college they went to or the celebrity they followed.

The results of the study revealed some interesting findings. First, the non-targeted advertisement was the least effective in generating clicks before and after the policy change. Before the policy change, the targeted non-personalized advertisements had the best click-through rate. After the policy change, however, the click-through rate of the targeted and personalized advertisements was almost twice as effective as before the change. Therefore, this change was highly significant and supported the findings that people are more willing to share their information if they feel in control [ALB20].

A drawback of this study is that there was no controlled change that caused the differences in response. Thus, there is a possibility that there were other factors than the change itself, such as the publicity surrounding the policy change. As with other studies, this study is somewhat outdated, as it was conducted in 2010. Both Facebook as a platform has changed since the experiment was conducted, and there possibly being a shift in public opinion.

This thesis builds on the work from previous studies. First, the online survey bases its questions on previous work, in order to get validated scales for the survey. In particular with regards to attitudes affecting user perceptions of privacy policies [ILRB21], the interpretation of technical terms in privacy policies [TSLB21], what affects users' willingness to share information with online advertisers [LUW+13] and the role of privacy fatigue in online privacy behavior [CPJ18]. The setup of the user experiment is particularly influenced by with the scenario based tasks studying the effects of different privacy adaption methods by Namara et al.[NSK22].

Chapter 4

Methodology

Given this background and previous research, this thesis aims to explore the user perspective of online privacy management, focusing on the research questions defined in Section 1.1. In order to get insight into the factors that might influence privacy management, it was beneficial to gather data from multiple sources using a mixed-method approach. This approach allows the combination of both qualitative and quantitative data [Cre09], which in this study was done by combining an online survey and a user experiment combined with an interview. I did this by using a sequential mixed-method approach, combining the findings in one method with the findings from another method [Cre09]. Releasing the online survey first made it possible to change the direction of the quantitative method based on the answers from the quantitative data. Additionally, it was a way of recruiting participants for the user experiment and interview. By combining these three methods, the results might be more accurate than they would otherwise have been.

4.1 Online Survey

Surveys can be used as a quantitative approach to gather information from a large sample of individuals. By using surveys, data can easily be standardized and potentially generalized to any population [RM16]. Making an online survey made it possible to gather information from a large group of people. This was time preserving, as there was no need to recruit respondents physically. Additionally, this made it possible for the respondents to be anonymous using the University of Oslo's data collection tool "Nettskjema.no", the most used and secure data collection tool in Norway [UniversityofOsloUiONettskjema]. This approach makes it easier for the respondents to answer more honestly while also avoiding answers influenced by interviewer bias [RM16]. However, this approach has some disadvantages, as it gives room for misunderstandings in the survey questions that the researcher might not detect [RM16]. Additionally, there is still a possibility that the respondents report the answers they see as "correct" rather than their actual beliefs or experiences.

Because of the nature of this study, the respondents might be inclined to report more privacy-seeking behavior than they truly have. An important measure for this thesis is to get an accurate depiction of what the respondents actually know and understand, as well as what they might find difficult. Because of this, the survey is not a reliable enough data source in itself, as it makes it difficult for the respondents to ask clarifying questions or elaborate on their answers.

The goal of the survey was to map how people manage their privacy online. The overall structure of the survey was; (1) personal questions, mapping who the respondents were, (2) knowledge-based questions, mapping overall privacy awareness, (3) thoughts on targeted advertising, (4) opinions and practices related to data privacy, (5) the use and knowledge of privacy-focused services, and lastly (6) what type of information they were willing to share with advertisers. The questions were selected to mainly answer Research Question 1, by mapping the respondents relationship with online privacy as well as Research Question 2, by getting some insights into privacy management strategies.

4.1.1 Question Selection

Most of the questions were based on related work to ensure that the questions were integrating validated scales. Additionally, this made it easier to get additional input on what is essential to consider when creating such a survey. The complete list of questions with sources can be found in Table 4.1. It is interesting to see how different kinds of people answer the survey. In "Why Should I Read the Privacy Policy, I Just Need the Service", mentioned in Related work 3 Ibdah et al. made a point system in which they gave a score based on how much they knew about privacy based on the information gathered [ILRB21]. This is where the question about password preference is taken from. From this idea, I also found it interesting to include some knowledge questions about the subject. I took all of these questions from "Defining Privacy: How Users Interpret Technical Terms in Privacy Policies" [TSLB21]. The options were also taken from this paper, as they were based on misconceptions people had about technical terms. A notable example is that there were no options for the question about third parties. This was because I wanted to see how people interpreted this term and if some misconceptions were notable. For the questions about targeted advertising, the first six questions were taken from "What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers" [LUW+13]. Some questions in the section on data privacy attitudes were taken from "The Role of Privacy Fatigue in Online Privacy Behaviour" [CPJ18]. Lastly, the different types of personal information were taken from [LUW+13].

Table 4.1: Survey Questions with References

Which of these passwords do you prefer to use?	Ibdah et al. [ILRB21]
In your understanding, which of the descriptions below best describe the purpose of a privacy policy	Tang et al. [TSLB21]
In your understanding, if you send a "Do Not Track request", are websites or apps able to track you?	Tang et al. [TSLB21]
In your understanding, when you are using a so-called "private browsing" window or "incognito mode" while surfing the internet, where is data from your browsing session stored?	Tang et al. [TSLB21]
In your understanding, what does it mean if a website uses third party cookies?	Tang et al. [TSLB21]
In general, I find targeted advertising useful	Leon et al. [LUW+13]
In general, I find targeted advertising distracting	Leon et al. [LUW+13]
In general, I find targeted advertising to be relevant to my interests	Leon et al. [LUW+13]
I usually don't look at the ads that appear on the websites I visit	Leon et al. [LUW+13]
Targeted advertising is necessary to enjoy free services on the Internet	Leon et al. [LUW+13]
I have clicked on an ad in order to get more information about the product	Leon et al. [LUW+13]
Targeted advertising is necessary to enjoy free services on the Internet	Leon et al. [LUW+13]
I am concerned that the information I submit to online vendors can be misused	Choi et al. [CPJ18]
I am tired of privacy issues	Choi et al. [CPJ18]
Would you be willing to share the following types of information with an advertising network?	Leon et al. [LUW+13]

4.1.2 Quality Assurance

The survey went through several iterations to ensure that it was as user-friendly and understandable as possible. After the initial first draft was finished, this version was reviewed by two classmates and one student of an unrelated subject. The feedback from this iteration was that the language was quite challenging, as the questions were taken from scientific papers. Additionally, there was a suggestion to have a Norwegian version of the survey, as most of the respondents in question would be Norwegian. Having this version of the questions would ensure that more people would be inclined to answer the survey. One of the test participants noted, "the answers have no value if they do not understand what they are answering". Thus, two versions were made both with more straightforward language than the original iteration. Two research assistants went through the English version in the second iteration, while one other went through the Norwegian version. Except for a few typos and changes in wording, the feedback from this run was positive. The final survey was opened to the public after this last iteration. The final English version of the online survey is included in Appendix A.

4.1.3 Distribution

The majority of the participants were a part of my personal network. I started by posting the survey link to SNSs such as Facebook and Instagram and direct messaging anyone I believed could be interested in answering the survey. The Facebook post was shared by four other people and posted on their personal Facebook walls. Some also reported sharing the link with colleagues and close friends. Additionally, I shared the link on an online bulletin board for project participation hosted by the university. On the first day, the survey reached about 80 participants. After three days, the link was shared on LinkedIn. After about one week, the survey reached a total of 128 participants; 107 answered the Norwegian version of the survey, while 21 answered the English version.

4.2 User Experiment and Interview

To comply with Research Question 3: *"To what extent do users perceive privacy settings of different companies as manageable?"* it was essential to have a data source that was not only based on self-reported thoughts in a survey, as respondents would possibly have vastly different experiences. Additionally, it would rely on a near-perfect recollection of their previous actions and experiences. Thus, I decided to have an approach that relied on a user experiment, in which every participant had to go through the same predefined tasks in a controlled environment. Through this, it was possible to accurately assess the participants' actual privacy management abilities through objective reference points (such as time-completion time) and give everyone the same reference point when assessing what aspects of privacy management they find difficult or time-consuming. To supply this data, an interview was conducted after each session.

By using interviews as a data source, the interviewer has the possibility to follow up on interesting answer and pick up on non-verbal cues from the participant [RM16]. Combining the interview with the user experiment gives a greater probability of understanding the complete picture of the participant's actions. The main drawback of using interviews as a data source is its time-consuming nature. In addition, there have to be enough participants in the study to get valid and generalizable results to some degree. The interview guide was limited to the most essential questions to combat this issue, giving each participant an average interview time of about 10 minutes.

The goal of the user experiment was to see how well the participants were able to navigate through settings related to privacy, data collection, and targeted advertising. Thus, it helped answer Research Question 3 (Section 1.1), by getting a look at the manageability of privacy settings. Additionally, the participants were interviewed after they completed the tasks about how they felt they did and their personal habits relating to the subject. This interview helped supplement the findings from the online survey, by allowing deeper insight in the responses. Thus, this part was also helpful in answering Research Questions 1 and 2 (Section 1.1). The advantage by having this approach is that it is possible to compare the responses given by the participants, with how they in reality solve the tasks. This allowed for a more robust data sample without worrying about the participants acting in a way that does not match what they report, as has been shown to be an issue in previous research [BN18].

4.2.1 The Setup

The websites were selected based the most used websites in Norway in 2021, the list was taken from similarweb.com [22a]. The focus of this study was on three of the most visited websites, google.com, facebook.com, and vg.no. Although youtube.com

is the second most visited website, it is also owned by Alphabet/Google, with privacy settings linked to a Google account, making it redundant to include in the study. Additionally, there is one task focusing on the settings in the browser, which in this experiment was Google Chrome as it is the most used browser as of 2022 [Sta22].

4.2.2 Creating "Ragnhild Paulsen"

It was important for all participants to have a neutral starting point without interference from personal preferences. Therefore, everyone completed the tasks on the same computer and the same accounts. By doing this, there was no need for the participants to have accounts on all of the sites, as well as it was easier to make sure the settings were the same before each participant completed the tasks.

The name was generated through a random name generator, behindthename.com [22b], with a setting for Norwegian names. A profile picture was used for the accounts to appear more realistic to the participants. This picture was randomly generated with AI using the site this-person-does-not-exist.com [22c]. In the Facebook information section, some details of her life were added, such as which university she had gone to as well as her relationship status. The profile is shown in Figure 4.1. All of the privacy settings were reset at a minimum for each session.

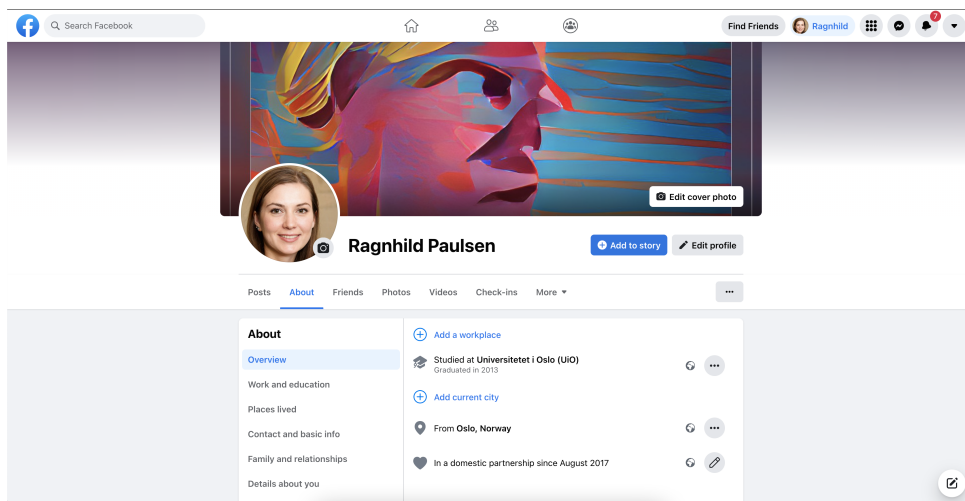


Figure 4.1: Facebook profile for Ragnhild Paulsen.

4.2.3 Tasks and Goals

The overarching goal of the tasks was to limit the information third parties could access about a person, with an extra focus on limiting online targeted advertisements. There were eight tasks in total, four of which were based on Facebook settings, two on the Google profile, one on Google Chrome (the browser used in the study), and one on VG. Facebook had the most relevant settings for the purposes of the study, and is, therefore, the largest contributor.

Between each task, the participants were asked to fill out a short survey on how they felt they completed the task. They were asked whether or not they thought they had completed the task and answered a few questions on how the settings were to use. The tasks were measured on three aspects; how easy the setting was to locate, how easy the user interface was perceived, and if they felt happy with the amount of time used to complete the task. These were based on work from Sauro and Dumas, and their use of post-task usability questionnaires in usability tests [SD09]. Additionally, screen recordings were used to measure completion time as a more objective indicator on how they did. The complete list of tasks and questions can be found in Appendix B.

Task 1: Limit who is able to see your profile.

Assuming most of the participants were somewhat familiar with all of the sites chosen for the study, the first task was chosen as something it would be plausible to believe they might have done before; limit the information available to people outside their network. Thus, the first task was to edit some privacy settings related to the visibility of the Facebook profile, as shown in Figure 4.2. This task had the least "obvious" answer, as it required multiple settings to be changed; therefore, all answers in which the participants restricted some settings in *Privacy* were marked as correct. Because the task was focused on the profile, participants who edited settings in *Profile and Tagging* also had the task marked as correct.

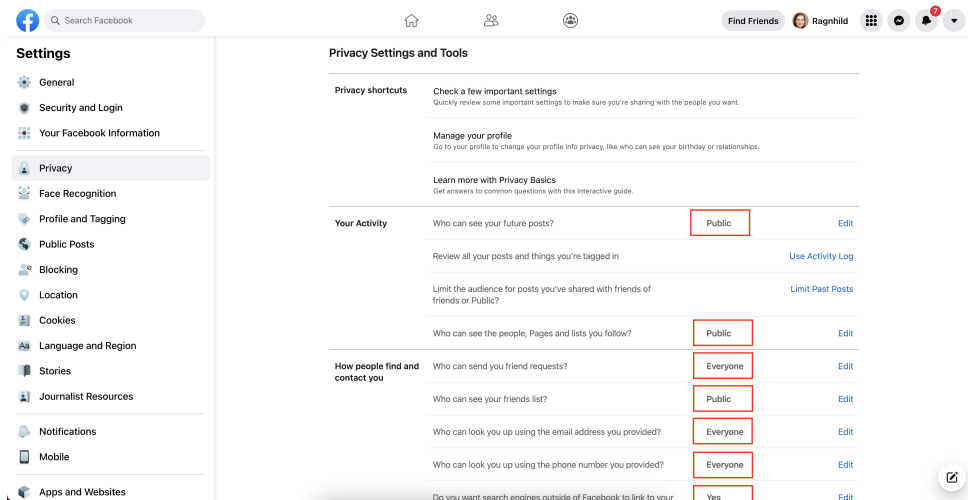


Figure 4.2: Settings for Task 1.

Task 3: You want to make it so Facebook cannot track what you do on other websites.

The goal of this task was to edit the cookie settings, without directly specifying this to the participants. One of the optional cookies that can be switched off allows Facebook to gather information from other websites to use on their sites. As long as this toggle shown in Figure 4.4 was switched off, the task was marked as correct.

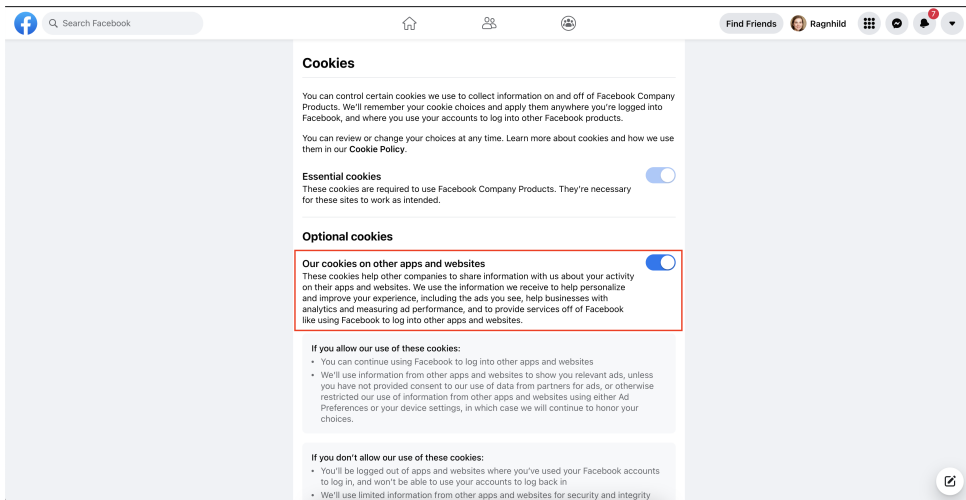


Figure 4.4: Settings for Task 3.

Task 4: Do not let Facebook use your information to advertise outside of Facebook.

This last task on Facebook is also based on the ad settings, as with Task 2. The goal was for the participant to locate the toggle button, which disallowed the use of their information for advertisements outside of Facebook (Figure 4.5). In order for the task to be marked as correct, the toggle had to be switched off.

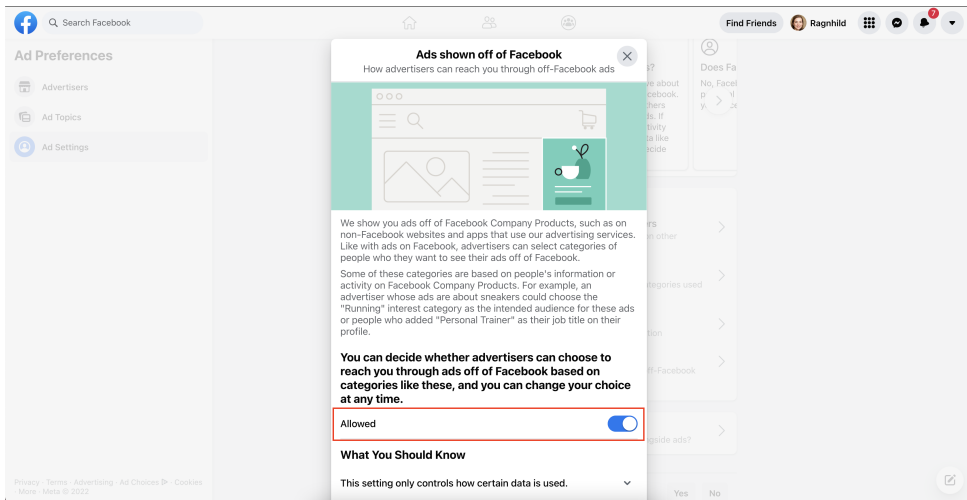


Figure 4.5: Settings for Task 4.

Task 5: You want to get an overview of the information Google uses to give you targeted advertising.

This task does not focus on a setting but rather on a page where the participants could see all of the categories Google used to reach "Ragnhild" with their advertisements (Figure 4.6). The goal was to locate this site and look at the collected information. The task was marked as correct as long as they found the right page; it made no difference whether or not they switched off personalized advertisements.

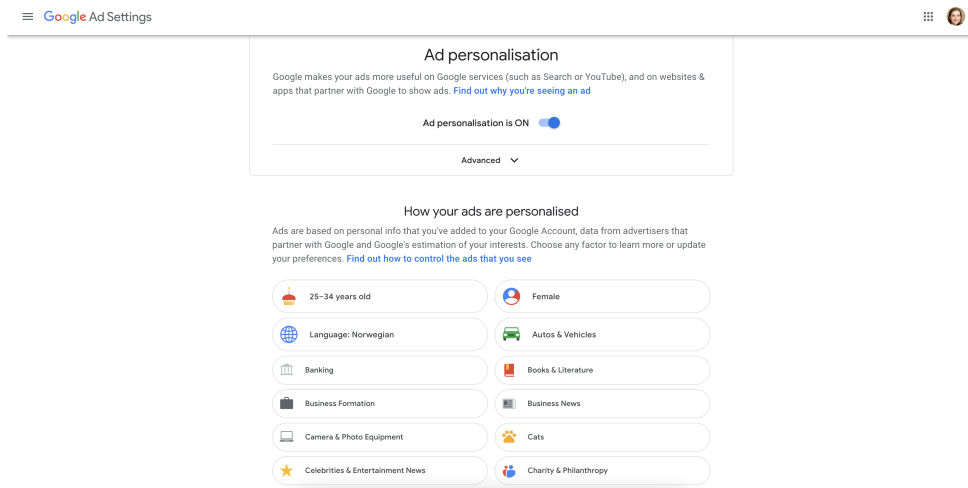


Figure 4.6: Settings for Task 5.

Task 6: You don't want your position to be used to give you any suggestions.

The goal of this task was to *pause* the location tracking on Google under *Data and Privacy* in the google account settings. This was done through the toggle button shown in Figure 4.7.

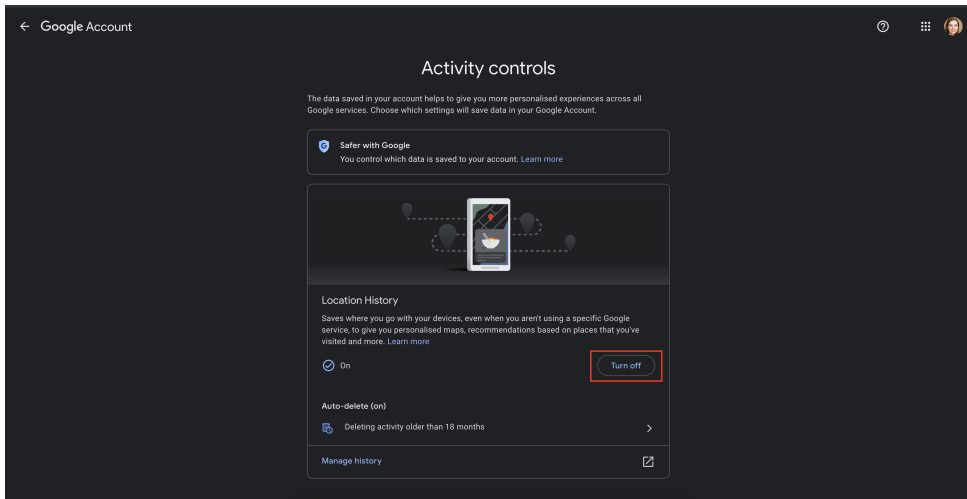


Figure 4.7: Settings for Task 6.

Task 7: You want your web browser "Google Chrome" not to allow third-party cookies.

In this tasks, the participants were asked to block all third-party cookies through their web browser (Figure 4.8). The task was marked as correct as long as they changed the cookie setting; there was no penalty for choosing the *Block all cookies* setting. However, this does cause the accounts to log off, making the next task impossible to do. Therefore, all of the participants who did this were asked to change it to the *Block third-party cookies* option afterward.

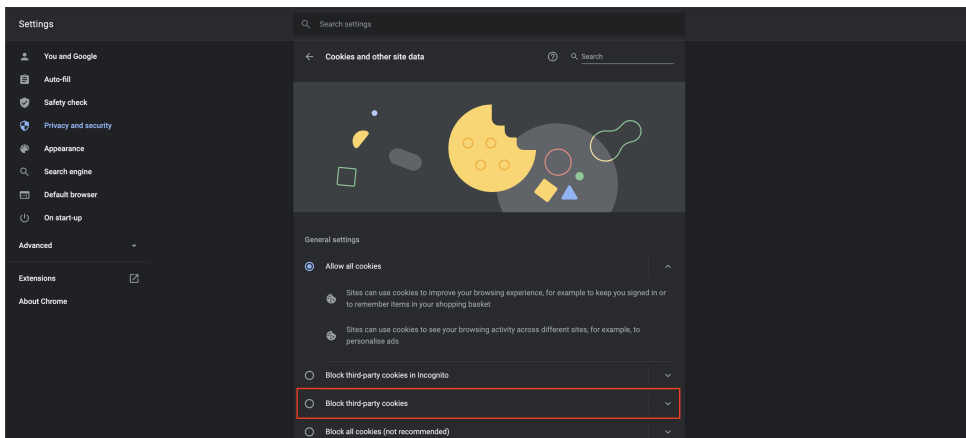


Figure 4.8: Settings for Task 7.

Task 8: Turn off targeted advertisements on VG

The goal of this task was to locate and turn off the settings for different targeted advertisements. These settings were located by going through the *Schibsted* account, a media group that owns many online newspapers in Norway. This task was approved if all of the toggles were switched off.

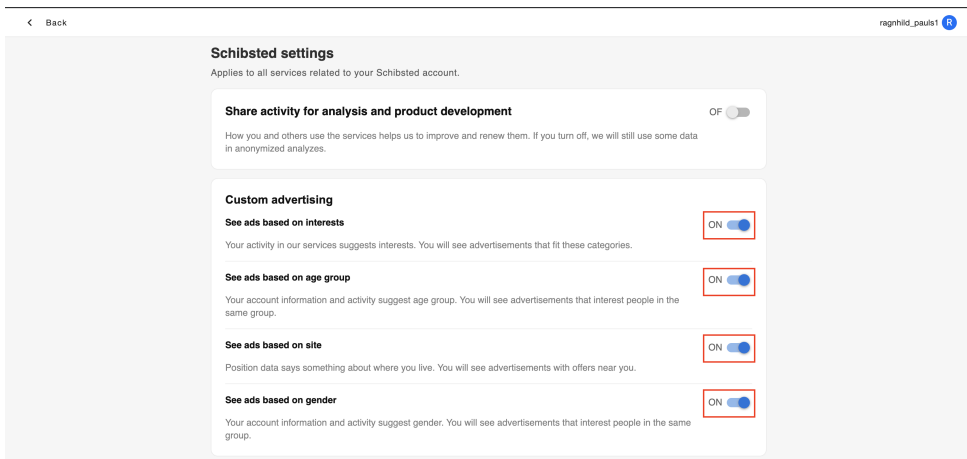


Figure 4.9: Settings for Task 8.

4.2.4 Accessing the Settings

Some settings had multiple possible solutions. The most straightforward paths to the settings related to the tasks are shown below.

Facebook

All of the tasks were possible to complete by accessing *Settings*. Facebook had organized the settings in a menu on the left-hand side of the screen. The correct categories are shown in Figure 4.10. *Ads* had their own preferences menu, where the participants had to click on *Ad settings* in order to solve Task 3 and Task 4, as shown in Figure 4.11. The correct categories in Ad settings are shown in Figure 4.12

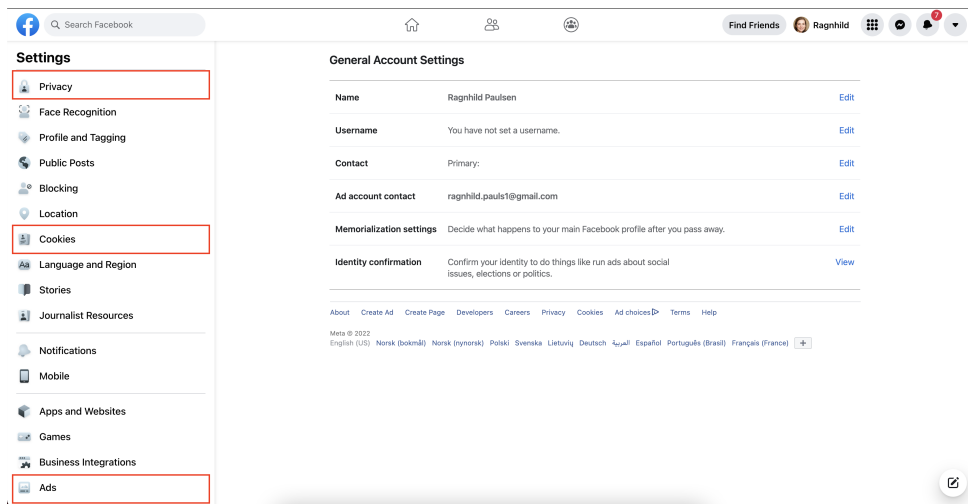


Figure 4.10: The relevant categories of Facebook settings.

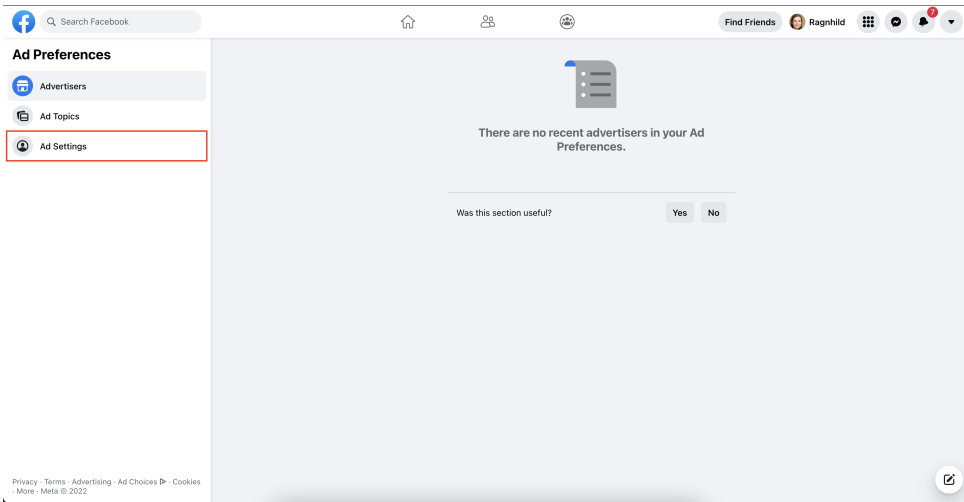


Figure 4.11: Facebook ad preferences.

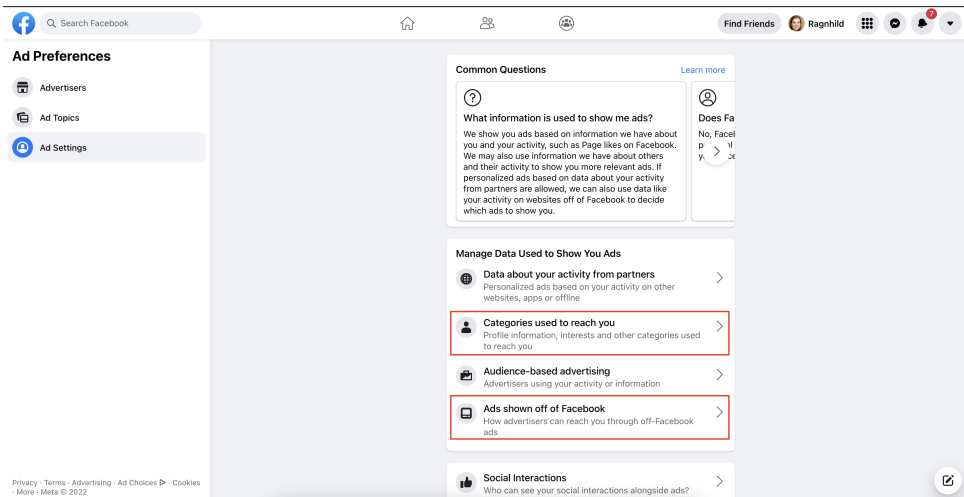


Figure 4.12: The correct categories of Facebook ad settings.

Google

The tasks for Google were all located under *Data and Privacy*, shown in Figure 4.13. Task 1 was completed by clicking *Ad settings*, while the page for editing the location data was located through *Location history*.

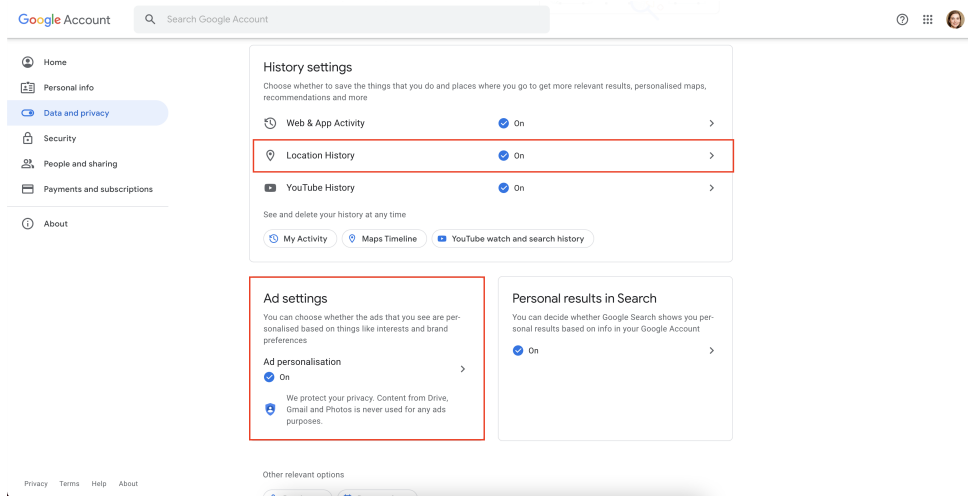


Figure 4.13: The correct Google settings under *Data and Privacy*.

Google Chrome

In order to turn off third-party cookies, the participant had to access the settings in the browser. This is shown in Figure 4.14.

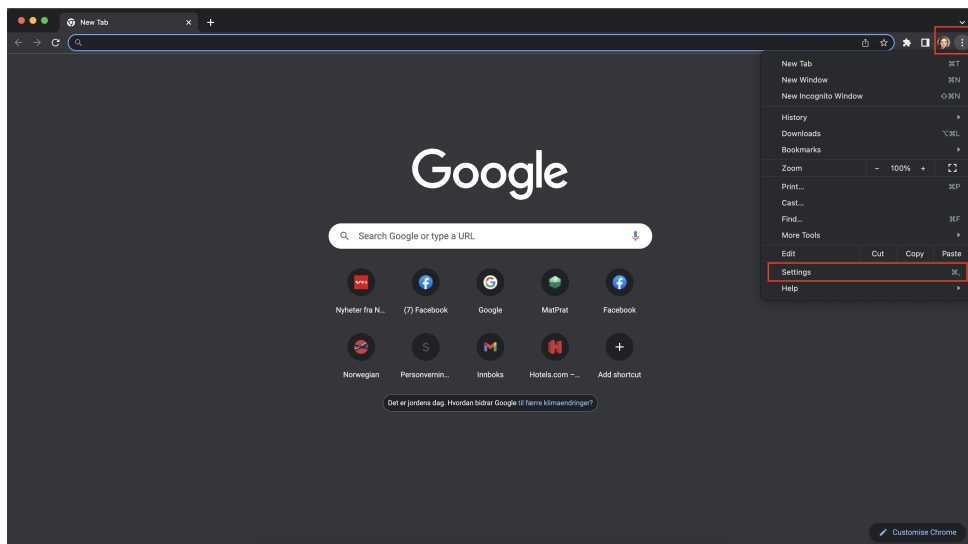


Figure 4.14: Where to access the settings in Google Chrome.

VG

The settings for ad management in VG were located under *Privacy policy*, as shown in Figure 4.15.



Figure 4.15: Where to access the VG settings.

4.2.5 Conducting the User Experiment and Interview

Each session was divided into two parts, one for completing the tasks and the other for answering questions about the tasks as well as personal experience and behavior. The participants were all given the same tasks in the same order. All of the sessions were at the end of March 2022.

Every session was conducted in the same private office provided by the IIK. The participants sat on one end of the table, with no one looking at their screen while they were going through the tasks to make the situation less stressful. However, they were encouraged to ask clarifying questions if they felt something was unclear about the tasks. They were not allowed to use any external search engines to find the correct settings. The setup included a MacBook Pro for completing the tasks, as well as a tablet for navigating through the tasks. The tasks were given to the participants one by one. The setup is shown in Figure 4.16.

The interview questions mainly focused on the tasks the participants had completed as well as the participants' own experiences and thoughts on online privacy management. The English version of the interview guide can be found in Appendix C. Recordings of the sessions were conducted on an Olympus Digital Voice Recorder (pictured in Figure 4.16).

4.2.6 Grading

Each session had a screen recording used to see if they did the tasks correctly and see how much time was spent on each task. The participants were told to move on if they spent more than 5 minutes on a task, therefore, anyone who was still going after 5 minutes did not get their attempt approved. Additionally, each participant was asked to close the tab between each task, making it easier to time the events. This also made it so that each task had the same starting point, making it harder to get hints from where they found the previous answer. If anybody forgot to close the tab, an additional 5 seconds was added to their time to make up for the time needed to access the site and settings. The clock started when the participant started moving their cursor and stopped when they pushed the correct button. If there were multiple buttons to be pushed, the timer stopped when the participant pushed the first button.

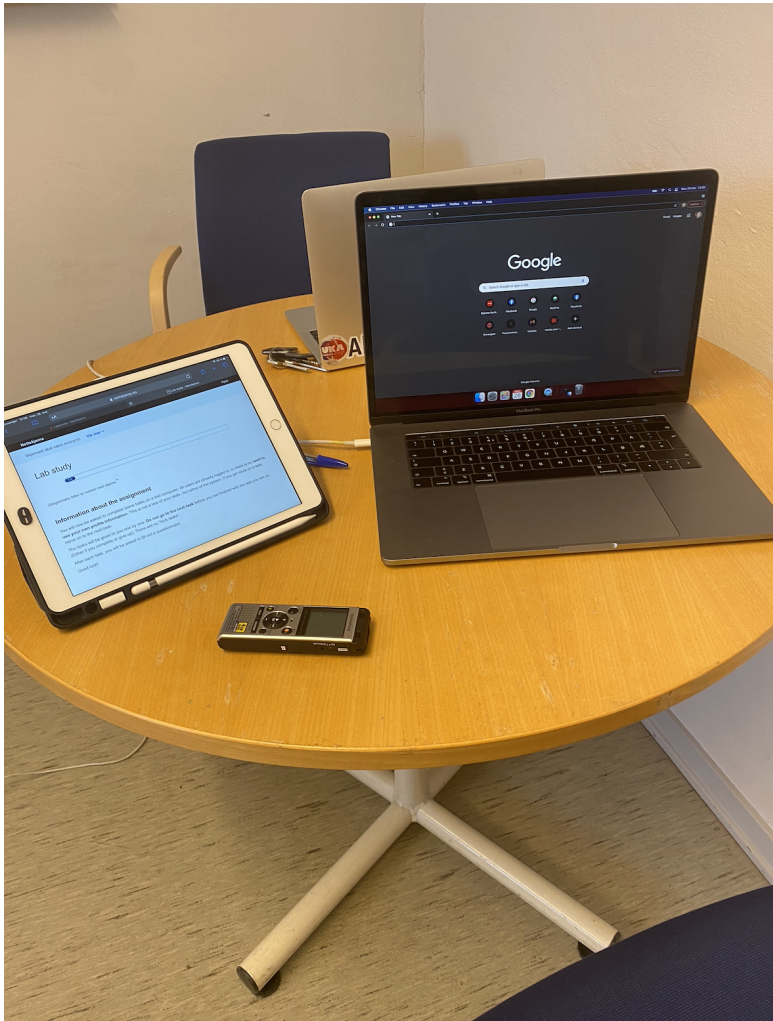


Figure 4.16: The setup for the user experiment.

4.2.7 Anonymity and Privacy

The project was approved by The Norwegian Centre for Research Data (NSD), and I handled the data in accordance with this agreement. All the participants were given an ID, which linked their identity through the physical consent forms they signed. No personal identifiers were stored in any other place. After transcribing the interviews, all voice recordings were deleted.

4.2.8 Limitations

There were a few limitations with the setup of the study. First, since two of the participants were not Norwegian, the survey had to be adapted for English. In order for Google Chrome to change its language, the machine had to be restarted, which was not done for one of the participants. Second, there were some issues with the translation tool used on the Norwegian site VG, which caused some language trouble. Additionally, the first participant who turned off *all cookies* instead of just *third-party cookies* in Task 7 (4.2.3), was not able to go back to change their cookie settings in order to complete the last task. This may have caused some of the participants not to get all the marks they might have otherwise gotten. Another source of confusion was the use of Google Chrome as a browser as it was easy to confuse with the Google account. Chrome was chosen because it is the most used browser, though it might seem like some of the confusion could have been avoided with a different choice.

4.3 Analysis

After the online survey and user experiment, the data had to be processed and analyzed. The results of the analysis can be found in Chapter 5.

4.3.1 Online Survey

The survey analysis was done using IBM SPSS Statistics (SPSS) and Excel. Excel was used to organize the data and create diagrams for the data. SPSS was used to do statistical analysis on the relevant variables. For each category: age, gender, education level, and Information and Communication Technology (ICT) background, the responses were compared. For the non-categorical questions, non-parametric tests were used to test the variables without any assumptions [Fie17]. Mann-Whitney tests were conducted for comparing two independent groups, while Kruskal-Wallis tests were used for multiple independent groups [Fie17]. For the categorical questions, χ^2 tests were conducted. All significant differences ($p < .05$) are reported in Section 5.1.

4.3.2 User experiment and interview

The user experiment and interview were analyzed separately. The results from the user experiment were combined with the self-evaluations to categorize the different types of answers, based on whether or not the participants were able to accurately say if they completed the tasks correctly. Additionally, Excel was used to make diagrams of all the results. NVivo was used to code the answers from the interviews and categorize the responses. The categories used were: *"what would make tasks easier"*, *"what was the most difficult"*, *"what keeps them from better privacy management"*, *what do they wish they had*, *"thoughts on targeted ads or data collection"*, *"strategies"*, *"privacy relationship"*, *"interface"*, *"how they felt it went"* and *"familiarity with settings"*.

Chapter 5

Results

This chapter is divided into three sections for each of the methods explained in Chapter 4. First, the results from the online survey are presented in Section 5.1. Second, the results from the user experiment are displayed in Section 5.2. Last, Section 5.3 displays some key findings and quotes from the interviews.

5.1 Survey

The results from the online survey are presented below, as well as the results from the statistic analysis on the responses. These results will be further interpreted and put into context in the Discussion (Chapter 6) and the highlights are briefly summarized at the end of this section.

5.1.1 Demography

The respondents were divided into different categories based on their age, gender, nationality, education level, and whether they were studying or had studied in an ICT-related field.

Most of the respondents were between the ages of 18 and 54, with 94.5% of the respondents being between these ages. The largest group of respondents were in the age group *18-24* with 40.6%. After this, the second largest group was aged *25-34* with 28.9%, age group *45-54* with 15.6%, and age group *34-44* with 9.4%. 1.6% of the respondents were under the age of 18, while 3.9% were over the age of 54. The distribution of age groups is shown in Figure 5.1.

The gender of the respondents is shown in Figure 5.2. 62% of the respondents were female, and 36% were male. 2% were non-binary or preferred not to say.

Figure 5.3 shows the highest completed education levels of the respondents. The largest group of respondents had a bachelor's degree or equivalent, with 53.9%. 22.6%

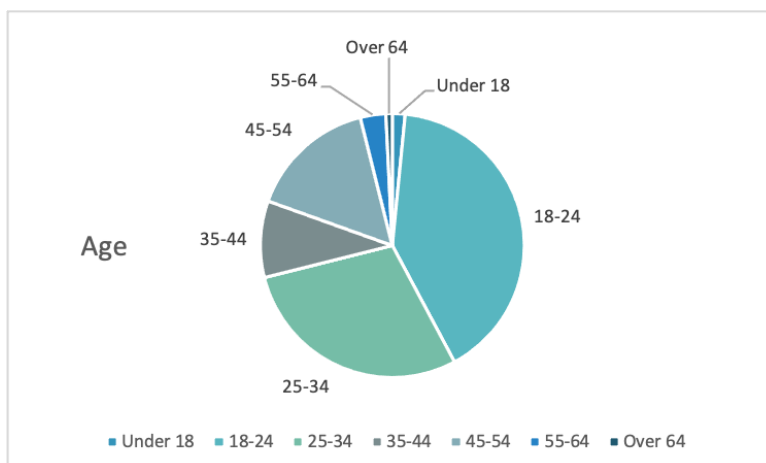


Figure 5.1: Age groups of the respondents.

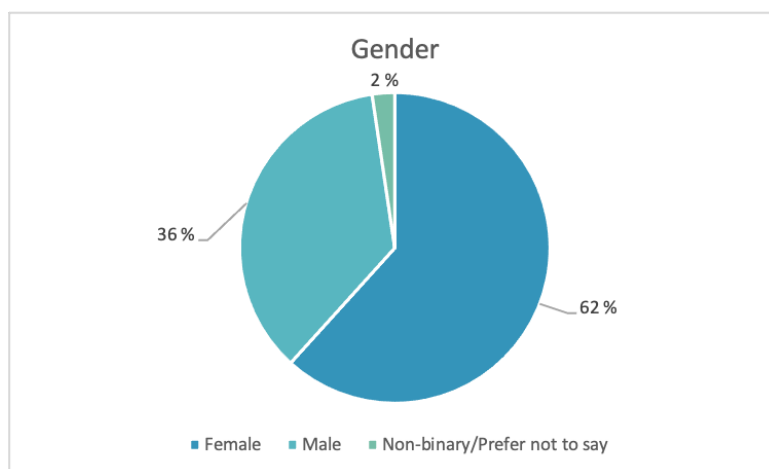


Figure 5.2: Gender of the respondents.

had some high school or completed high school as their highest education level, which was relatively equal to the number of respondents with a master's degree or higher, which was at 23.4%.

The nationality of the respondents is shown in Figure 5.4. The largest group of respondents reported being Norwegian, making up 85,9% of the respondents. Out of the about 14% non-Norwegian respondents, 12.5% were from another European country, while 1.6% were from a non-European country.

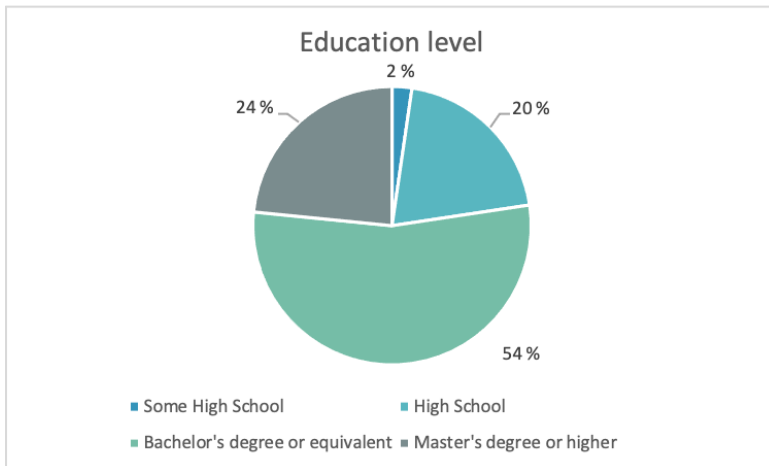


Figure 5.3: Education level of the respondents.

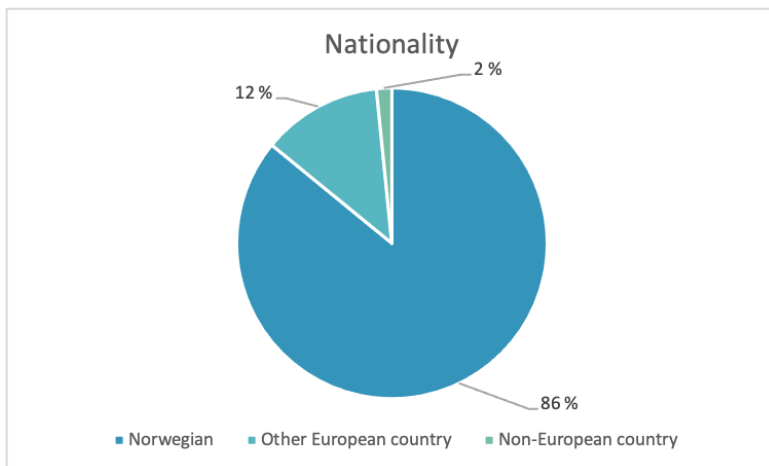


Figure 5.4: Nationality of respondents.

66% of the respondents reported studying or having studied in an ICT-related field (Figure 5.5).

5.1.2 Questions on Terms

The participants were quizzed on the meaning of different terms relevant to online privacy. On the question "What is the purpose of a privacy policy" 71.1% of the respondents answered correctly, while 45.3% of respondents answered that websites

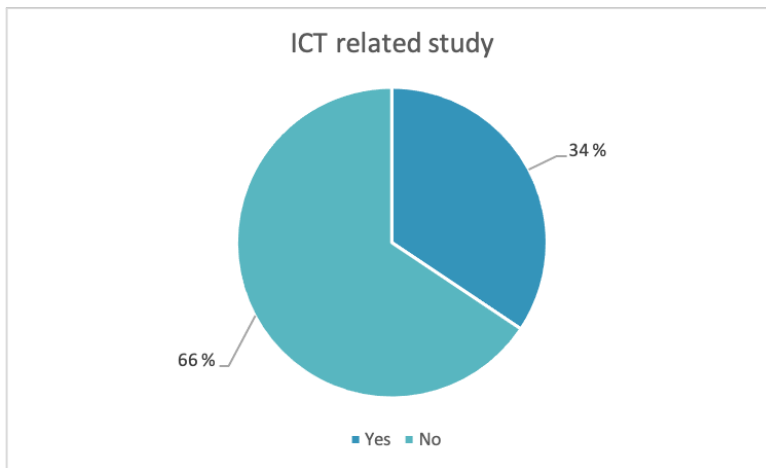


Figure 5.5: ICT-related background among respondents.

and apps were able to track them if they sent a "Do Not Track" request. The responses to these questions are shown in Figure 5.6.

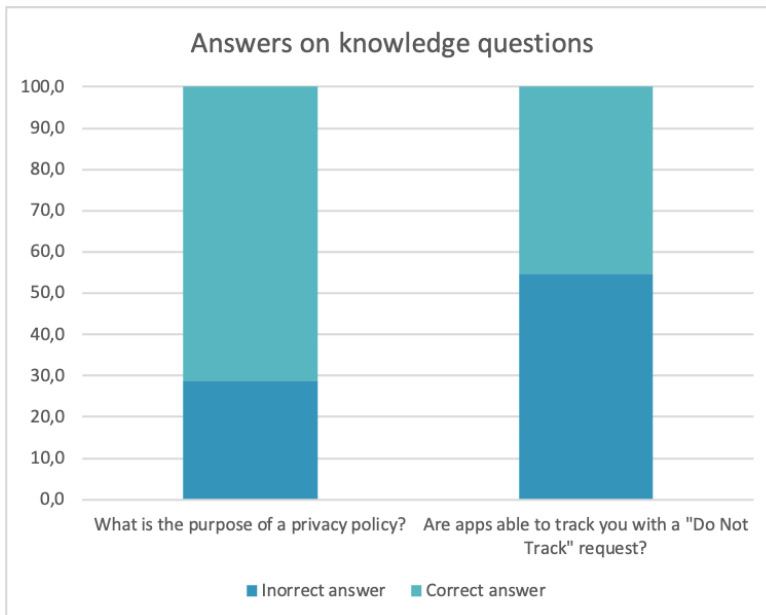


Figure 5.6: Correct and incorrect answers to knowledge questions.

On the question of where session data is stored in private browsing, 48.4% were

able to choose at least one correct answer. The responses for all options are shown in Figure 5.7, with the correct responses highlighted in green. 48.4% of the respondents knew that session data is stored on the websites' machines or servers, while 34.4% knew that the data could also be stored on the machines or servers belonging to third parties.

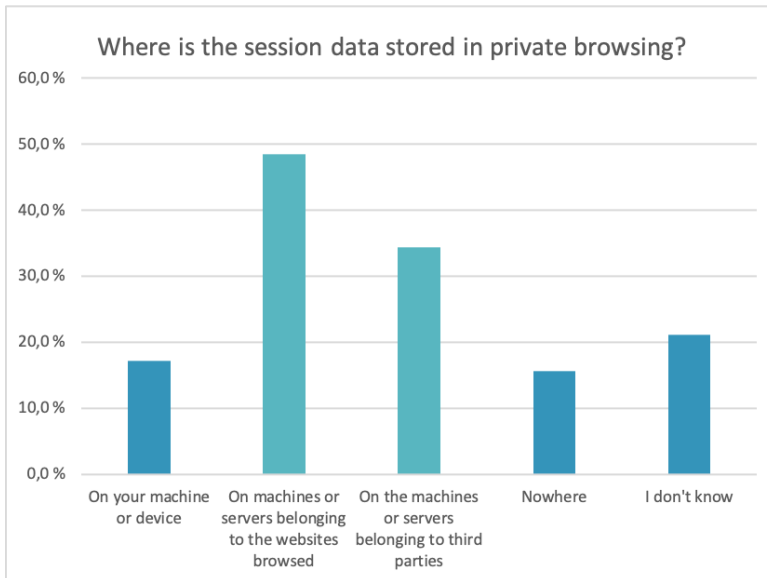


Figure 5.7: Answers to where session data is stored in private browsing.

The questionnaire (Appendix A) also included an open question about third party cookies and 23% of the respondents were able to produce an answer that was close to the correct answer. The correct answer is something similar to "Third parties set cookies on the website you are visiting in order to track your movements on this site". In order for the answer to be marked as correct, it needed to be clear that they meant third parties inserted a cookie to track their information on that site. The results are shown in Figure 5.8. Other than "I don't know", there were two common answers to this question. The first was that many thought it was the opposite of what it is, meaning that they thought the websites use third party cookies to personalize the site itself. The second misconception was that that many did not know the difference between third party cookies and first party cookies, and believed it was important for the functionality of the site.

Additionally, the respondents were asked to pick the most similar password to the password they would prefer to use out of a list of options (Figure 5.9). The most popular option was "aa123456@", with 38.3% reporting that they would prefer this option. 34.4% wanted to pick the most difficult password: "jbdkfdjll34904@*Ed4G2+",

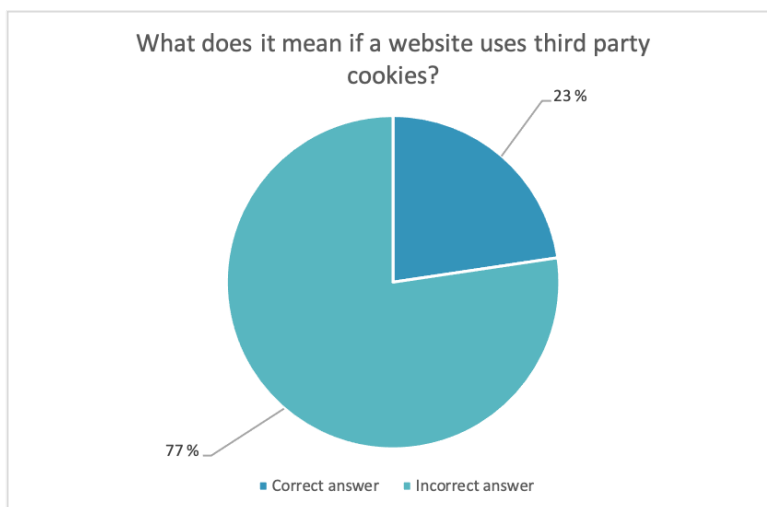


Figure 5.8: Answers to what third party cookies are.

while 19.5% wanted "acidanthera" as their password. Only 3.9 % would choose the weakest password "football".

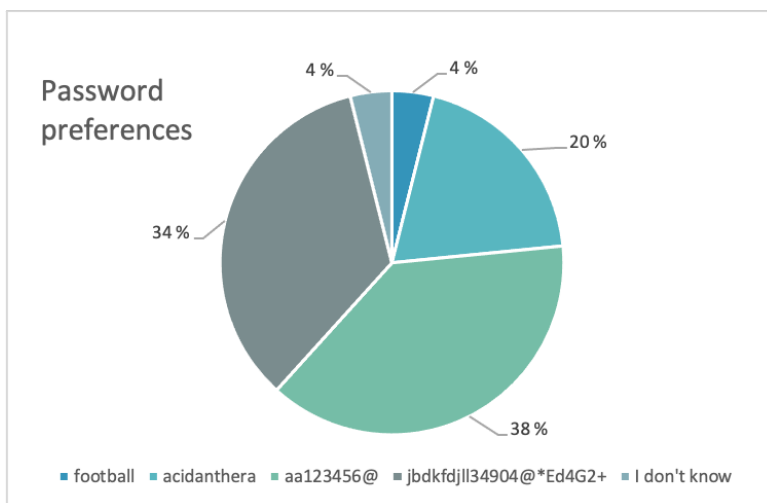


Figure 5.9: Responses on password preferences.

In order to determine whether or not there were significant differences between the groups in terms of password choices and general knowledge of key terms, χ^2 tests were conducted. These tests revealed that gender and education level had no significant influence on the respondents' password choices or on whether or not the

respondents answered the questions correctly. In terms of age, the respondents under the age of 35 were significantly more likely to know what the purpose of a privacy policy is ($\chi^2(3)=15.617, p = .001$). Further, the respondents with a background in ICT were more likely to choose the most difficult password as their preferred password ($\chi^2(3)=15.974, p = 0.001$). There was no significance for any of the groups for the question on third party cookies.

5.1.3 Targeted Advertising

Figure 5.10 shows the respondents' thoughts on targeted advertising. 32% of the respondents either *agreed* or *strongly agreed* with targeted advertising useful, while 39.1% *disagreed* or *strongly disagreed* and 28.9% were *neutral*. 40.6% *agreed* or *strongly agreed* that targeted advertising is necessary to enjoy free services on the Internet. 71.1% reported having *agreed* or *strongly agreed* they had clicked on ads in order to get more information. 72.6% reported that they sometimes were scared by targeted advertising, with 44.5% *agreeing* and 28.1% *strongly agreeing*.

The statistical analysis of differences in these attitudes in terms of gender, education level, age, and ICT background or not also revealed a number of interesting nuances. First of all, a Kruskal-Wallis test indicated a relation between the attitude towards targeted advertising and education level ($H(2)=8.604, p < .05$). As post-hoc test procedure, separate Mann-Whitney tests were conducted, using a Bonferroni correction to the alpha level (.008). These indicated that participants with a Master's degree or higher are significantly less likely to find targeted advertising useful than those with a high school diploma as their highest education level ($U=265, p = .008$). In terms of potential gender differences, Mann-Whitney tests indicated that men indicated to a greater extent than women report that they do not look at ads that appear on websites they visit ($U=1421, p < .05$). Additionally, women were more likely to click on ads ($U=1377, p < .05$) as well as being more likely to click on targeted ads on their smartphones than on their computers ($U=1099, p < .001$). Women also reported that they were more scared of targeted advertising than men ($U=1182, p < .001$). In terms of differences between respondents with and without a background in ICT, the ICT participants were less likely to look at ads that appear on websites ($U=1357, p < .05$). A Kruskal-Wallis test showed a relationship between the respondents' age and whether or not they had clicked on an ad in order to get more information on a product ($H(3)=15.519, p < 0.05$). A post-hoc Mann-Whitney test with a Bonferroni-correction to the alpha level (.008) indicated that the age group "35-44" was less likely to click ads than the age group "under 24" ($U=152.5, p = .008$) as well as the group of "25-34" ($U=65, p < .001$ (not corrected for ties)).

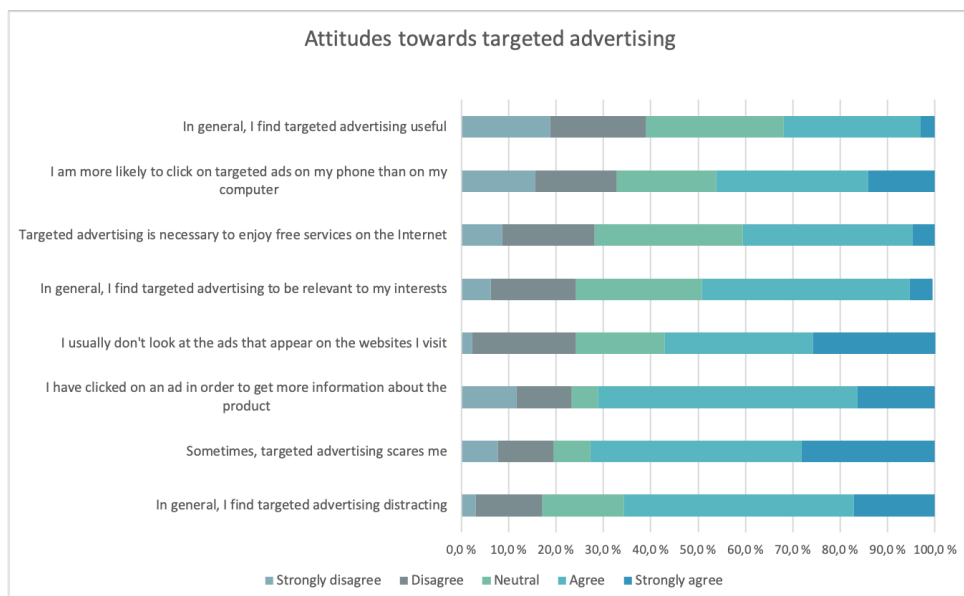


Figure 5.10: Attitudes towards targeted advertising.

5.1.4 Privacy

Figure 5.11 shows the responses from the section on privacy attitudes. 64.8% of the respondents were concerned that the information they submitted to online vendors would be misused, and 63.3% were concerned that the information they had shared online would be exploited. Furthermore, over 8 out of 10 respondents (84.4%) reported being mindful of the information they shared on social media, with 45.3% reporting they *agreed* and 39.1% reporting they *strongly agreed*. Another 82% of the sample *disagreed* or *strongly disagreed* with the statement "I don't care what happens to my data". On the statement "I know how the information I shared is being used" 79.7% either *disagreed* or *strongly disagreed*, while 8.6% reported that they *agreed* or *strongly agreed*. 7.8% reported finding it easy to manage their online privacy, while 77.3% *disagreed* or *strongly disagreed*. 64.8% reported having trouble finding the privacy settings they wished to edit.

Mann-Whitney tests revealed some differences relating to privacy attitudes when comparing the different groups. In terms of gender differences, men reported that they took more active measures to manage their privacy than women ($U=1425$, $p < .05$). They also reported that they changed their default privacy settings more than the women did ($U=1347.5$, $p < 0.02$), while women reported that they felt more powerless in their privacy management ($U=1357.5$, $p < .02$). In terms of ICT

respondents, the ICT respondents were more concerned with what happened to their data ($U=1297$, $p < .02$), while the non-ICT respondents reported that they read privacy policies before accepting them more than the ICT respondents ($U=1238$, $p < .02$). The non-ICT respondents also reported that they found managing their online privacy easier than the ICT participants did ($U=1419$, $p < 0.05$). The analysis also showed a relationship between age and reading privacy policies ($H(3) = 40.722$, $p < 0.05$) as well as whether or not they had avoided signing up for a service because of the privacy policies ($H(3)=16.243$, $p < 0.05$). Using a post-hoc Mann-Whitney test with a Bonferroni correction to the alpha level (.008), the age group "35-44" were more likely to read privacy policies than both "under 24" ($U=79.5$, $p < .001$ (*not corrected for ties*)) and "25-34" ($U=60$, $p < .001$). The same was true for the "over 45" group, with them being more likely to read the privacy policies than the "under 24" ($U=217$, $p < .001$) and "25-34" ($U=161$, $p < .001$ (*not corrected for ties*)). The age group "24-34" also reported having avoided signing up for services more than their younger counterparts ($U=537.5$, $p < .001$).

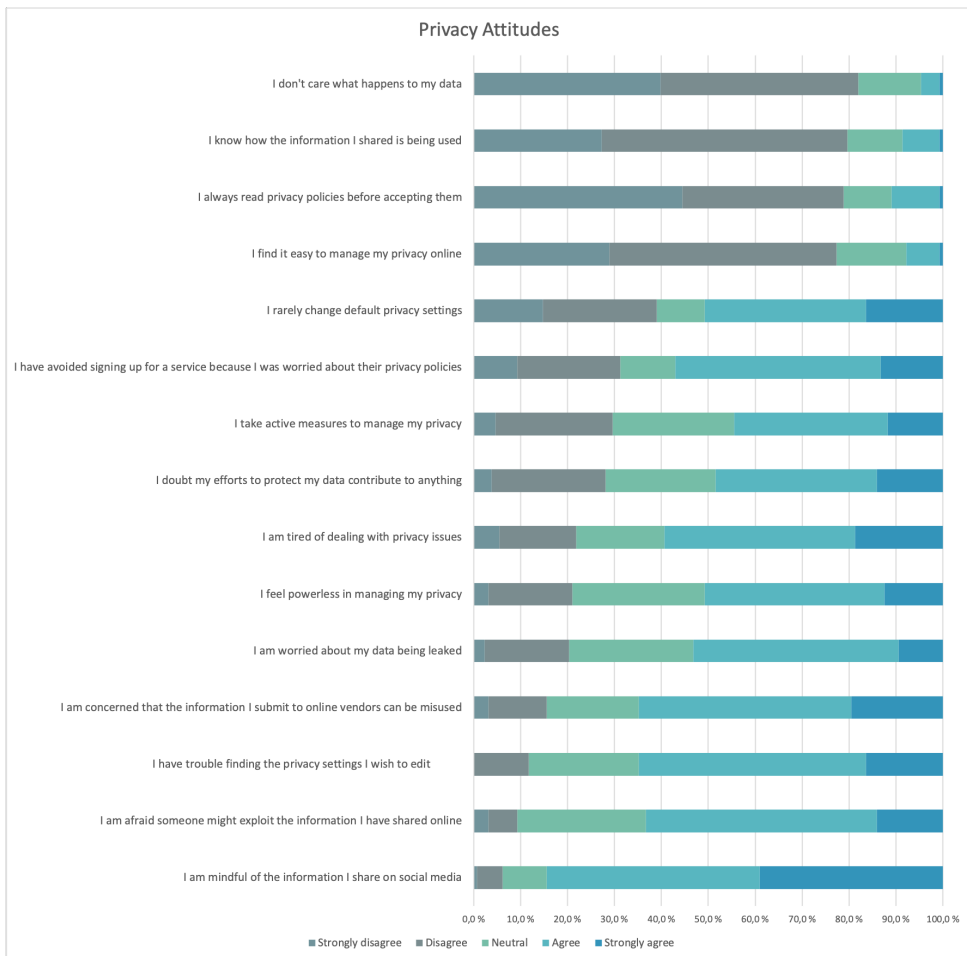


Figure 5.11: Responses on privacy attitudes.

5.1.5 Privacy Focused Services

Figure 5.12 shows the percentage of the respondents who have heard of different services. The blue answers are the respondents who have heard of the service but do not use it, while the green answers are the respondents who also use the services in question. The two services most of the respondents had heard of were VPN and Two Factor Authentication (2FA), with 91.4% and 84.4%. 2FA was used by almost all who had heard of it, with 98% of the respondents who had heard of it using the service. 76% of the respondents who had heard of VPN also used the service. The service that was least familiar among the respondents was the instant message

service Signal, with 24.2% having heard of it. 42% of the respondents who had heard of the service also used it. The service which was the least used was the Tor browser, with 6.2% of all respondents using it or 14% of the respondents who had heard of it using it.

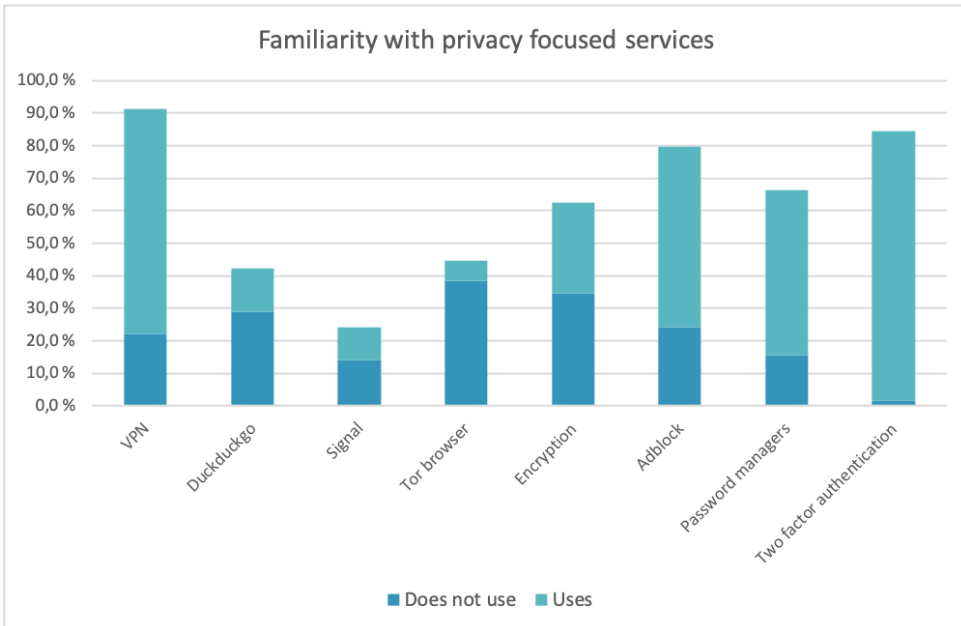


Figure 5.12: How many of the respondents had heard of the different services.

The respondents were also asked to report how often they used the services, which is shown in Figure 5.13. Two-factor authentication is the service that is used the most on a daily basis, with 49.2% of the respondents. 36.7% of the respondents reported using Adblock services daily and 35.9% used password managers daily. 70.8% of the respondents who reported using password managers did so daily. Tor browsers were used daily by 0.8% of respondents and 12.5% of the Tor users, which was the lowest for any of the services. VPN was the second most used service, with 20.3% using the service daily, 22.7% using it weekly and 26.6% using it monthly. The biggest hurdles for using the mentioned services are shown in Figure 5.14, showing that user friendliness and difficulty to manage these services are the biggest hurdles for using them.

A series of χ^2 tests were conducted to check whether there are differences between the groups of interest in the use of privacy focused services. Overall the tests showed that men were more likely to use privacy focused service, with them being

significantly more likely to use Duckduckgo ($\chi^2(1)=8.053$, $p < .02$), encryption services ($\chi^2(1)=14.191$, $p < .001$), and Adblock ($\chi^2(1)=4.374$, $p < 0.05$). In terms of age, the younger respondents (<35) were significantly more likely to use Adblock ($\chi^2(1)=18.647$, $p < .001$) and VPN services ($\chi^2(1)=4.714$, $p < 0.05$). Having a ICT background also made an impact on what services the respondents used. The ICT respondents were significantly more likely to use VPN services ($\chi^2(1)=14.572$, $p < .001$), encryption services ($\chi^2(1)=10.261$, $p = .001$), password managers ($\chi^2(1)=10.924$, $p < .001$), and two factor authentication ($\chi^2(1)=7.295$, $p < .02$). Education level had no significant impact, according to these tests.

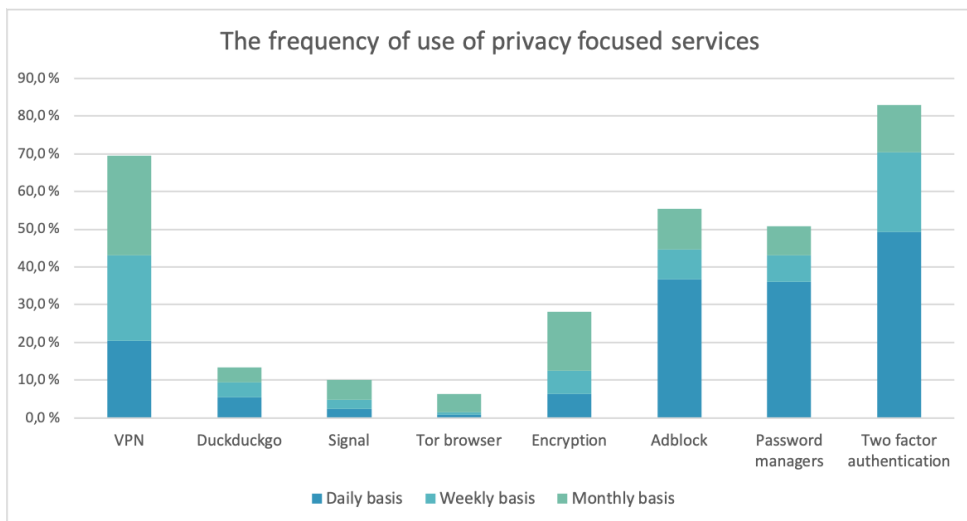


Figure 5.13: How often the respondents used the different services.

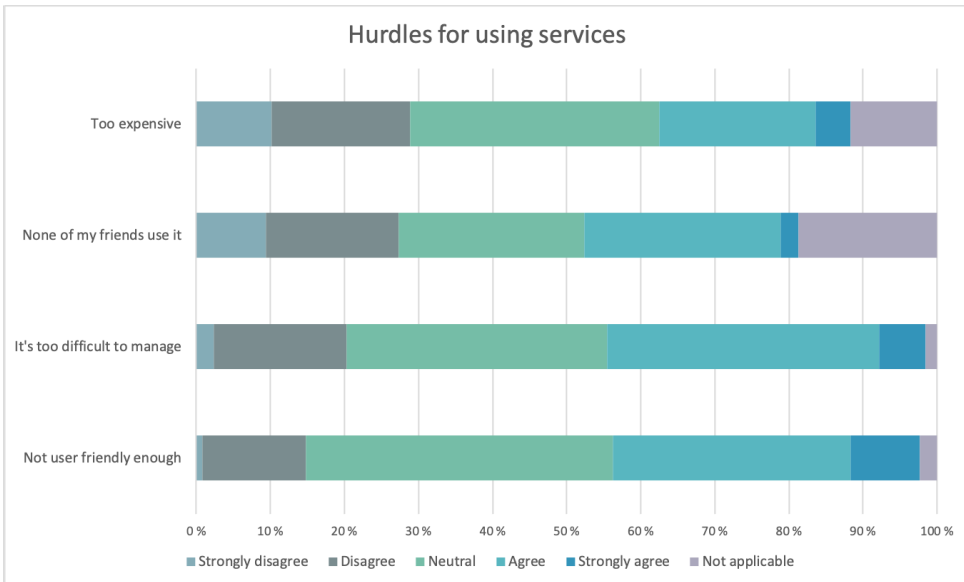


Figure 5.14: Hurdles for using privacy-focused services.

5.1.6 Willingness to Share Information with Advertisers

Figure 5.15 shows how willing the respondents were to share different types of information with advertisers. The respondents were least willing to share credit card number (0.0%) and social security number (1.6%), and most willing to disclose their gender (62.5%), age (50.8%) and operating system (39.1%). The respondents were most uncertain in whether or not they would allow advertisers information about their location (24.2%), email address (23.4%) and operating system (23.4%).

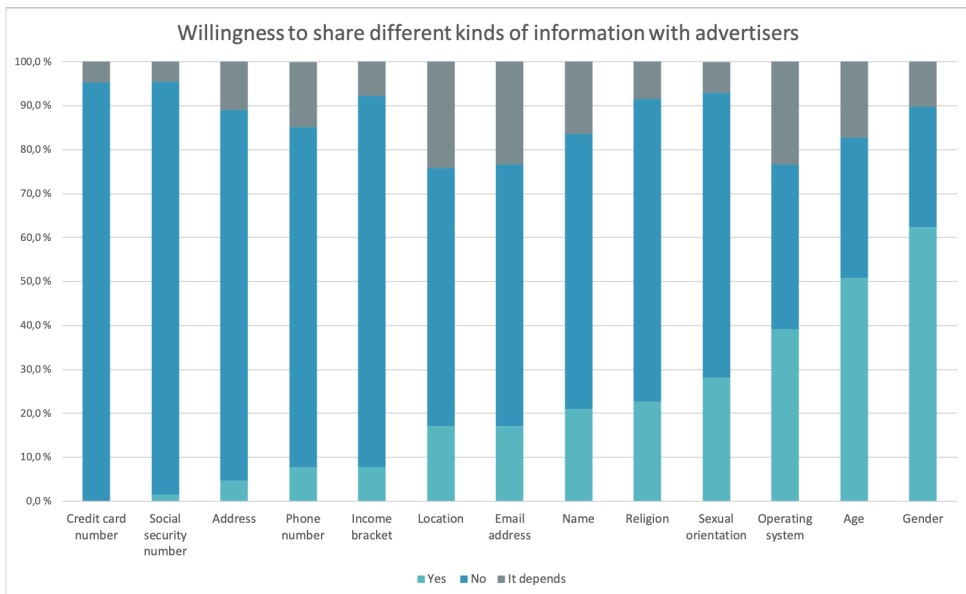


Figure 5.15: Willingness to share information with advertisers.

Highlights from the Online Survey

- Most respondents had some knowledge of privacy terms.
- Most of the respondents found targeted advertising to be scary and distracting, although a majority also reported having clicked on ads.
- > 80% reported caring about what happens to their data.
- Most respondents found it difficult to manage their privacy and were uncertain what their information is being used for.
- About half the respondents reported changing default privacy settings, while less than half reported actively managing their privacy.
- Half of the respondents felt powerless in managing their privacy, and a majority had trouble finding the settings they wished to edit.
- For the privacy focused services, VPN, 2FA and Adblock were used the most, while Signal and Tor browser were used the least.
- The biggest hurdles for using these services were user friendliness and difficulty.

- The majority of respondents were not willing to share sensitive information with advertisers.
- Women were less likely to take active measures to manage their privacy, while also feeling the most powerless in privacy management.
- Men were less likely to click on ads than women.
- Respondents with a Master’s degree were less likely to find targeted advertising useful.
- ICT respondents were more concerned with what happened to their data, and found privacy management more difficult than the respondents without an ICT background.
- Different groups used different privacy focused preferences.

5.2 User Experiment

The results from the user experiment are shown below. Both the correct answers, as well as the results from the self-report questionnaire between the tasks are presented.

5.2.1 Correct answers and times

The results of the user experiment are shown in Figure 5.16, the times are in minutes and seconds. On average, each participant was able to complete 5.25 (66%) of the tasks. See Section 4.2.3 for detailed explanations of the tasks. 16 of the participants (80%) were able to complete Task 1, making it the task with the most correct answers. Task 4 was the most difficult task for the participants, with 8 participants (40%) being able to complete this task. On average, each task was completed by 13.13 (66%) of the participants, with a median of 13.5. The average time to complete a task was 1 minute and 30 seconds. The participants spent the most time completing Task 6, with an average time of 1 minute and 58 seconds, while Task 8 required the least amount of time with an average of 58 seconds to complete the task. There were a total of $8 \times 20 = 160$ responses.

Participant	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6	Task 7	Task 8
1	01:08	01:59	02:43	02:03	03:27	03:50	00:30	01:20
2		00:15	00:59	03:01	03:36	01:08		01:21
3	01:28	03:30	00:40				01:16	01:11
4	01:07	01:26				01:20	03:17	00:47
5	00:38	02:07	00:40		00:48	00:39		00:56
6	00:58		00:24			00:31	01:18	
7				03:11	02:00	03:30	00:55	01:24
8			00:28		00:27	00:37		
9	01:03	00:33	01:23			04:50		01:03
10	01:28					04:03		01:05
11		00:55	02:22	00:25	00:38			00:40
12	01:25				00:18	00:36	03:05	00:39
13	01:45	01:39		00:40			03:02	00:17
14	02:28	01:19		00:30			00:21	
15	00:41	04:52		00:39	04:39	01:39	00:28	
16	00:59	01:25	00:28		02:30		00:18	00:28
17	01:02		00:48	00:50	01:48	01:00	01:21	00:44
18	01:37		00:57		01:24	02:16	00:56	
19	02:13		03:36			03:23	02:01	01:50
20	04:50	01:54	00:26		00:40	00:18	00:27	00:53

Figure 5.16: Results from the user experiment.

5.2.2 Participants

There were 20 participants in the user experiment. Some were selected after indicating interest in the project after completing the online survey (Section 4.1). Half of the participants were female, while the other half were male. All of the participants were between the ages of 21 and 26, with an average age of 23.8 and a median age of 23. Most of the participants were university students, with 17 being full-time students and three participants working full time. 18 of the participants completed the tasks in Norwegian, while two of the participants were foreign exchange students who were given an English version of the tasks. 11 of the participants were studying ICT-related fields. Five of the women and six of the men were studying in ICT related field, while five of the women and four of the men were not. As an incentive to participate in the user experiment, each participant was given a universal gift card valued at 200kr. Figure 5.17 shows which categories the participants fit under, while Figure 5.18 shows the gender distribution of the ICT and non-ICT participants.

Participant	Age, gender, ICT/non-ICT
1	26, male, ICT-student
2	23, female, non-ICT
3	23, female, ICT-student
4	23, female, ICT-student
5	25, female, ICT-student
6	26, male, non-ICT
7	25, male, ICT-student
8	25, female, ICT-student
9	25, female, non-ICT
10	23, female, non-ICT
11	22, male, ICT-student
12	23, female, ICT-student
13	24, female, non-ICT
14	23, male, ICT-student
15	26, male, non-ICT
16	21, male, ICT-student
17	21, male, ICT-student
18	23, female, non-ICT
19	23, male, non-ICT
20	26, male, non-ICT

Figure 5.17: The age, gender, and background of the participants.

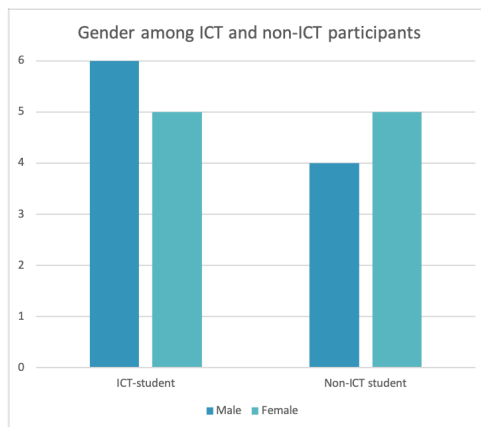


Figure 5.18: The gender distribution of participants with and without an ICT background.

5.2.3 Differences Between the Participants

The two main variables that have been differentiated between are gender and whether or not they were studying in ICT-related fields, as the ages were similar. Figure 5.19 shows the total number of correct responses for each task with gender, while Figure 5.20 shows the total number of correct responses with the field of study.

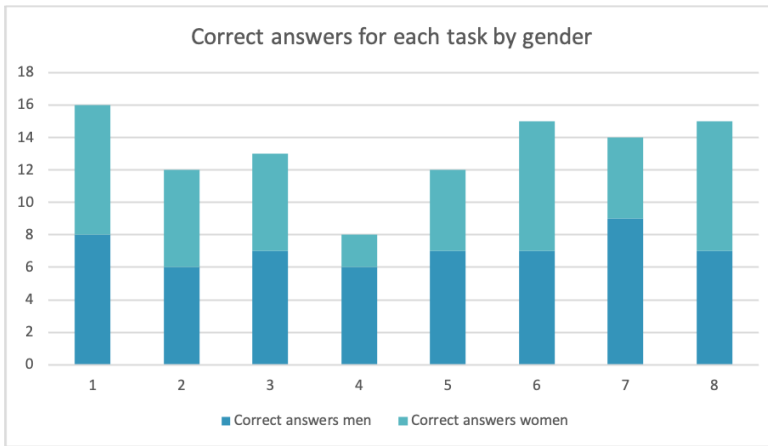


Figure 5.19: The correct responses for each task with gender.

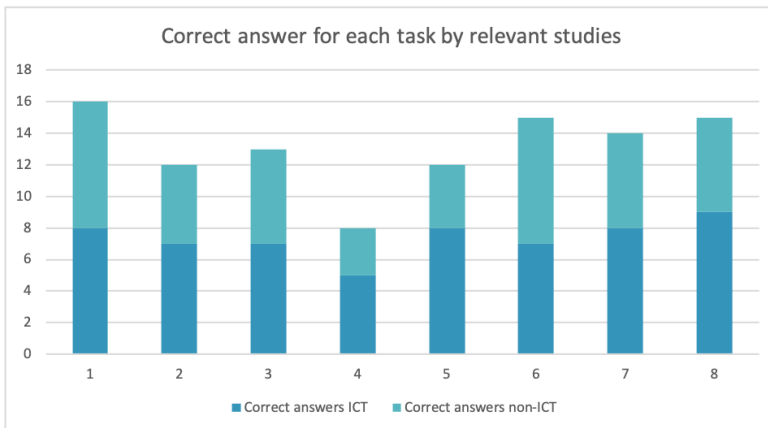


Figure 5.20: The correct responses for each task with relevant fields of study.

On average, men were able to complete 71% of the tasks, while women completed an average of 60% of the tasks. This constitutes 5.7 correct tasks for men and 4.8 correct tasks for women. The median of correct answers was 5.5 for the men and 5 for the women. Among the men, the highest score was 8 out of 8, while it for the women was 6 out of 8. 3 out of 8 was the lowest score for women, while the men had the

lowest score of 4 out of 8. The percentages can be seen in Figure 5.21. Overall the men were more likely to complete most tasks. Two of the tasks were equal between the genders, while men had more correct answers on four of the tasks. Task 4 had a noticeably large difference, with only 20% of women completing, while 60% of the men were able to do so. Task 7 also had a large discrepancy, with 90% completing this task, and 50% of women finding the solution. Women were marginally better at completing Task 6 and 8, with 80% against 70% on both of these tasks.

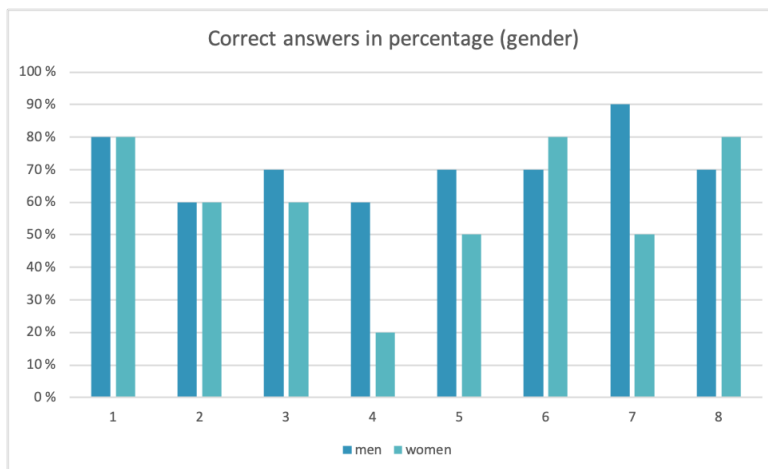


Figure 5.21: The correct responses with percentage for gender.

The participants studying ICT-related fields had an average correct task completion of 67%, while non-ICT participants completed 64% of the tasks. This constitutes an average of 5.4 completed tasks for participants with a background in ICT and 5.1 for participants without this background. Both groups had a median of 5 out of 8 correct answers. The highest score of an ICT participant was 8 out of 8, and the lowest was 3 out of 8. For the non-ICT participants, the highest score was 7 out of 8 and the lowest was 3 out of 8. The participants with an ICT background answered more accurately on five of the tasks, while the non-ICT participants had more correct answers in percentage in three tasks. Task 5 had the largest differences between the groups, with 73% of the ICT participants having completed the task, while 44% of the non-ICT participants answered correctly. The task which was answered correctly by the largest amount of non-ICT participants was Task 6 with 89% having the correct solution, against 64% of the ICT participants.

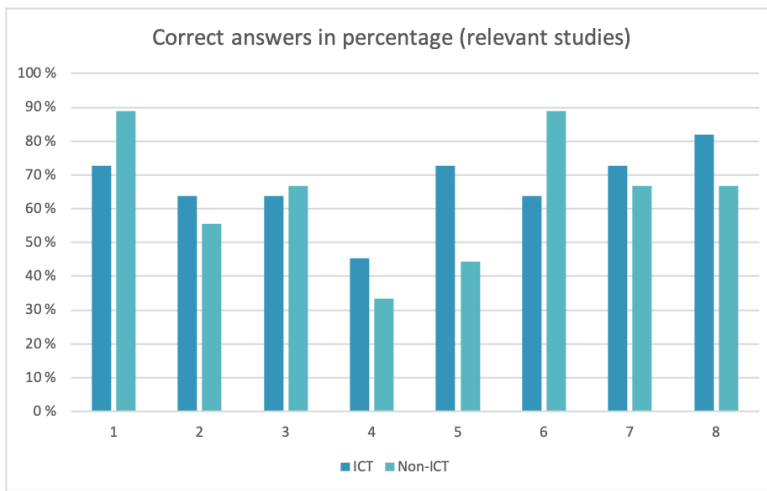


Figure 5.22: The correct responses with percentages for relevant fields of study.

5.2.4 Accuracy of Self-Evaluation

All of the participants were asked to assess their efforts in completing each task. There were five categories of responses, based on the results and the self-evaluation. First, a *correct yes* (green) entails the participants reporting that they were able to complete the task and this to be correct. A *correct no* (blue) is that the participants did not think they completed the task, and this is correct. An *incorrect yes* (yellow) entails the participant reporting that they were able to complete the task without actually doing so. If the participant did not think they complete the task, even though the screen recording showed that they did do it correctly, it is marked as *incorrect no* (purple). Lastly, all the tasks in which the participants were uncertain about whether or not they completed the tasks correctly are marked as *uncertain* (light blue). There are a total of 79 *correct yes* responses, 18 *correct no* responses, 20 *incorrect yes* responses, and 3 *incorrect no* responses. Additionally, there were 40 *uncertain* responses. The distribution is shown in Figure 5.23.

Figure 5.24 shows all the tasks with the different categories of responses. Task 8 had the largest amount of *correct yes* responses, with 75% of the participants fitting into this category. The task with the fewest *correct yes* responses was Task 4, with 30%. Task 1 was the only task without any *incorrect yes* responses, though it was also the task with the most uncertainty (50%). Task 2, Task 3, and Task 4 all had 20% of the participants in the *incorrect yes* category. There were rather few *incorrect no* responses, with only three in total, two of which were on Task 3.

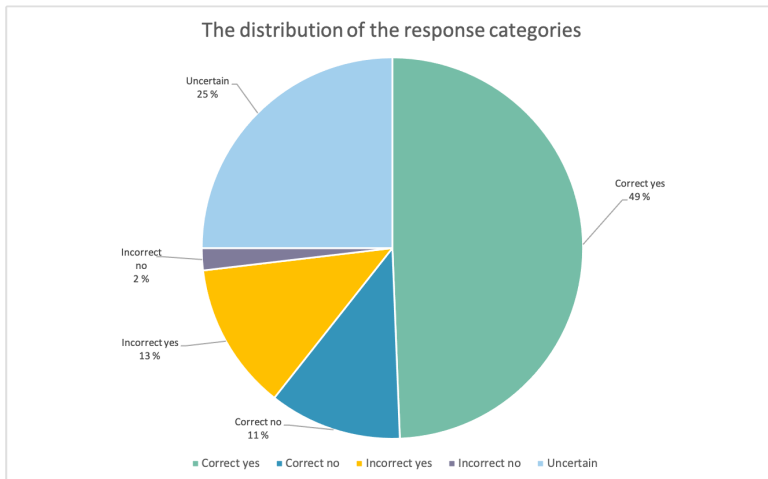


Figure 5.23: The distribution of the response categories.

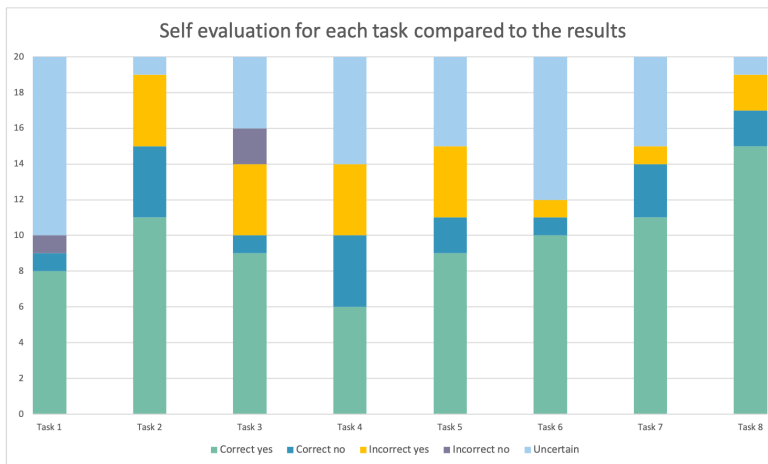


Figure 5.24: Correctness of self-evaluation for each task.

In Figure 5.25, the distribution of the different categories for each participant is shown. One of the participants had eight *correct yes* responses, which was the highest amount in this category of all the participants. The lowest amount of *correct yes* responses was one. The highest amount of *incorrect yes* responses was four, while five of the participants had no such responses. Two of the participants had no uncertainties in their answers, while the rest had at least one. The most uncertain participant reported being uncertain for five of the tasks.

Figure 5.26 shows the percentage of each gender in the total amount of answers

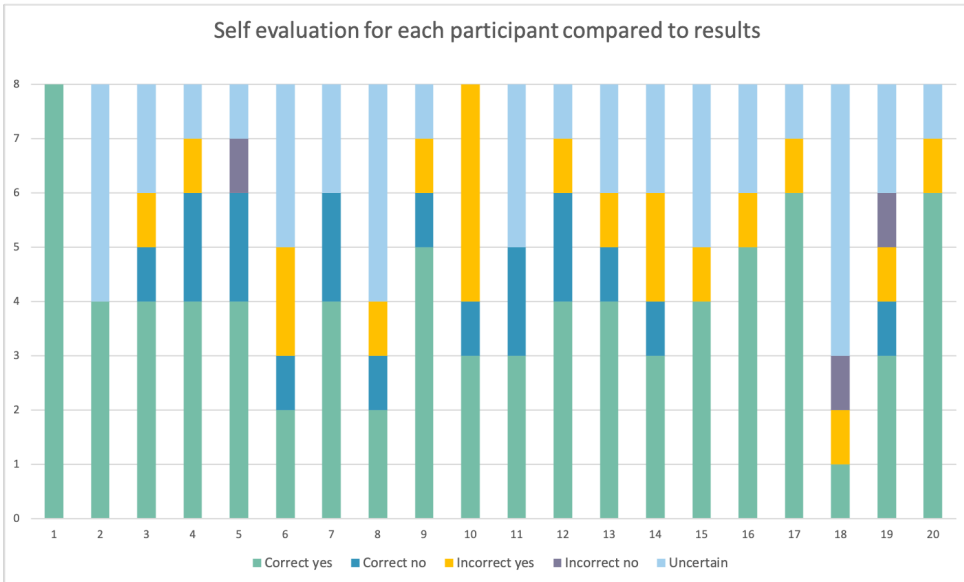


Figure 5.25: Correctness of self-evaluation for every participant.

in each category. Men had 56% of the *correct yes* responses, while women had 61% of the *correct no* responses. The largest difference between the genders is in the *incorrect no* category, where 67% of this category was from women. The *incorrect yes* category had a slight majority of women with 55%. The *uncertain* category was relatively equal with a 5% difference between the men and women.

Figure 5.27 shows the percentage of ICT and non-ICT participants in the total amount of answers in each category. The ICT participants had the largest amount of *correct yes* responses, with 59% of this category. As with the genders, the amount of uncertainty is relatively equal with 48% of the answers coming from ICT students, and 53% coming from non-ICT participants. The largest discrepancy between the two groups is in the *correct no* category, with 72% of these responses coming from the ICT participants. Similarly, the non-ICT participants have the largest amount of *incorrect yes* (60%) and *incorrect no* (67%) responses.

5.2.5 User Perception

For each of the tasks, the participants were asked to take a position on three claims relating to user-friendliness. The results of this are shown in Figure 5.28, Figure 5.29 and Figure 5.30.

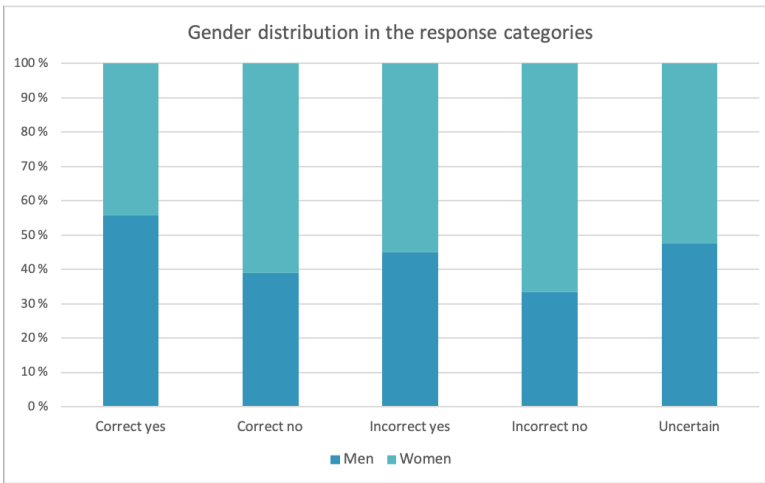


Figure 5.26: The percentage of the responses given by the genders in the different categories.

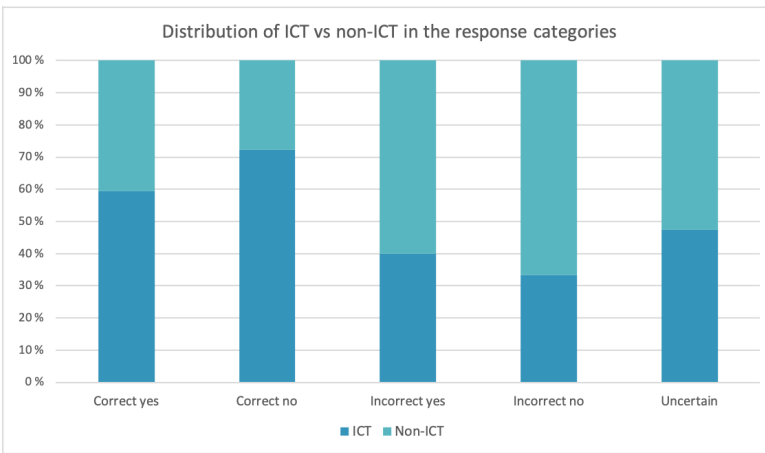


Figure 5.27: The percentage of the response given by ICT and non-ICT participants for each category.

For each task, the participants were asked if they found the setting easy to locate (Figure 5.28). The easiest task to locate was Task 8, with 60% saying they either *agreed* (55%) or *strongly agreed* (5%) with the setting being easy to locate. The most difficult task to locate was Task 4, with 70% reporting that they either *disagree* (35%) or *strongly disagree* (30%) with the statement. On average, 34% of the participants either *agreed* or *strongly agreed* that the tasks were easy to locate, 14% were *neutral* and 52% either *disagreed* or *strongly disagreed*.

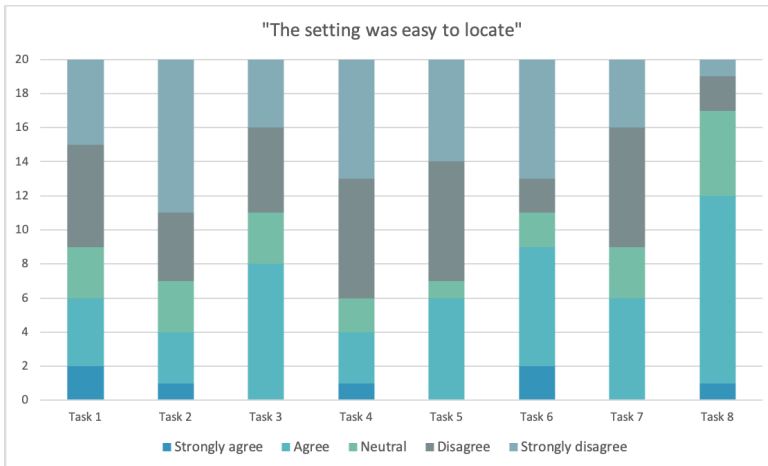


Figure 5.28: The responses to the claim: "The setting was easy to locate".

Second, the participants were asked to assess whether the UI was easy to use (Figure 5.29). The easiest UI was, according to the participants, Task 8, with 65% reporting they found they either *agree* (55%) or *strongly agree* (10%) with the statement. 50% of the participants found that Task 6 had a difficult UI, which was the lowest percentage for this statement. On average, 46% of the participants either *agreed* or *strongly agreed* that the UI for the task was easy to use, 23% were neutral, while 31% either *disagreed* or *strongly disagreed*.

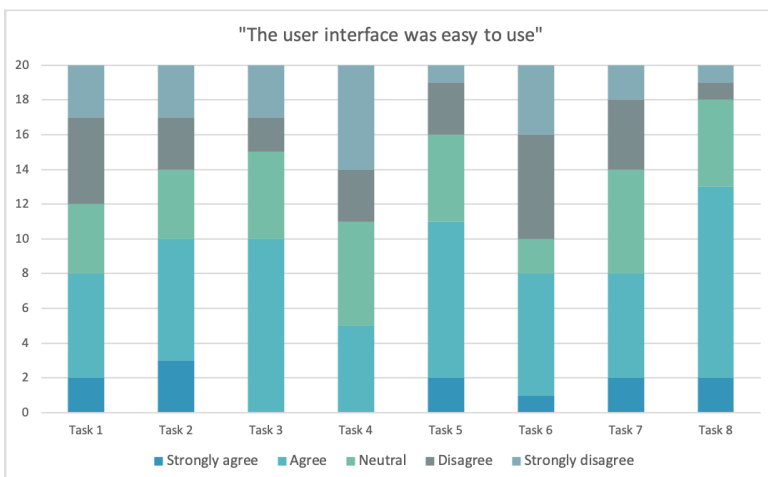


Figure 5.29: The responses to the claim: "The user interface was easy to use".

Lastly, the participants were asked to assess the amount of time they spent on

completing the task (Figure 5.30). 15% of the participants reported that they *strongly agreed* that they were happy with the amount of time they spent on Task 8, while 45% *agreed* with the statement. Task 3 also had 60% stating that they either *agreed* (55%) or *strongly agreed* (5%) that they were happy with the amount of time they used. The task the participants were the least happy with their time was Task 1, with 80% either reporting they *disagreed* (35%) or *strongly disagreed* (45%) with the statement. On average, the participants reported *agreeing* or *strongly agreeing* with being happy with their time for 39% of the tasks, 14% were neutral and 46% were unhappy with their time.

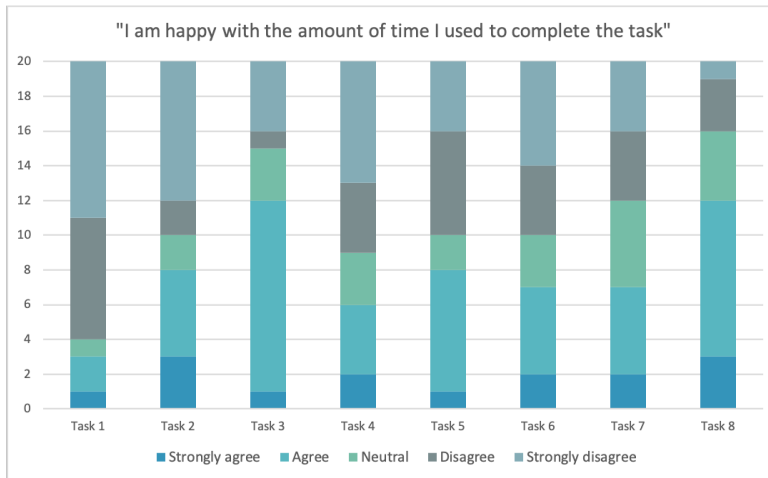


Figure 5.30: The responses to the claim: "I am happy with the amount of time I used to complete the task".

Highlights from the User Experiment

- On average, the participants were able to successfully complete 66% of the tasks.
- Task 1 had the most correct responses, while Task 4 had the fewest.
- Participants spent the most time completing Task 6, and the least time completing Task 8.
- Men were able to complete more tasks than the women, and ICT students completed more tasks than the non-ICT students.
- 49% of the responses were correct yes responses, 25% were uncertain, 13% were incorrect yes, 11% were correct no, while 2% were incorrect no responses.
- Task 1 and Task 4 were perceived as the most difficult, while Task 8 was perceived as the easiest task.

5.3 Interview

The participants of the user experiment were interviewed on their experience with completing the tasks and their thoughts on online privacy, based on the questions in the interview guide (Appendix C). The answers have been divided into different categories. For the part of the interview related to the tasks, there are five categories; how they felt it went, what was the most difficult aspect of the tasks as well as what could have made it easier, their thoughts on the user interface, and their familiarity with the settings. In the general section of the interview, the categories are; their relationship with online privacy, which strategies they have for managing their privacy, the barriers which keep them from protecting their privacy, and what they wish existed to make their privacy management easier. Most of the answers have been translated from Norwegian to English.

The age, gender, and background of the participants can be found in Figure 5.17.

5.3.1 How Did They Feel Like it Went?

Table 5.1: Summary of how they felt it went

They were uncertain if they did it correctly
It was harder than expected
It went fine

This was the first question the participants were asked, and the first response they thought of is what was recorded for this category. See Table 5.1 for a summary of the most common answers. Nine of the participants reported that they felt like they did not do well, six of the participants said that they felt like it went okay, while five reported that they felt like they did well on the tasks. Many of the participants reported feeling confused, stupid, and uncertain if they completed the tasks as they were supposed to. One girl, who felt like she did okay even though she was confused said:

"I felt like I went through all of the settings that were relevant, and still, I felt like I didn't find what I was looking for" - Participant #13

Another participant, who reported that he did well on the task himself, did not think that the tasks necessarily were easy to complete.

"I was thinking, while I went through the tasks, that my mom would never be able to locate this if she had tried"- Participant #16

5.3.2 What Was the Most Difficult Aspect of the Tasks?

Table 5.2: Summary of what the participants found the most difficult

There were too many possible paths
There was too much text to read through
It was hard to determine if they found the correct setting

A summary of the most common answers can be found in Table 5.2. Some reported the most difficult aspect to be one of the sites they visited in general, while others had more general difficulties such as *navigating through menus*. 12 of the participants said that they found Facebook to be the most difficult website, three said that Google was the most difficult, and two found VG to be the most difficult. Some noted that it was difficult to make sure that everything was turned off, such as one girl noted:

"More often than not, there is not just one button that turns off everything, you have to go through and make sure you have located all the buttons. That makes it difficult" - Participant #9

Many of the participants who found Google to be the most difficult task all went through *Privacy* instead of *Manage your Google Account*. One participant complained:

"The most difficult part was Google. When you found the correct site, it was possible to understand what they meant, but you had to read through an entire website with information to find a link." - Participant #1

In general, there were many complaints about too much text and difficult navigation on multiple tasks.

"There was a lot of information to read and it felt like searching through a labyrinth." - Participant #10

On Facebook, the participants found it difficult to navigate through the menus and locate the correct information. Additionally, some complained that the categories were not descriptive enough:

"There were so many categories, and multiple things fit in the same categories. Additionally, I felt like they don't want me to locate the button." - Participant #16

5.3.3 What Could Have Made it Easier

Table 5.3: Summary of what the participants felt could have made the tasks easier

Fewer tabs and categories
A search option in the settings
More of the settings located in one place

There were multiple things that many of the participants suggested would have made the tasks easier to complete, see Table 5.3. First, the most suggested thing was that the settings should have been collected in one place.

"They could have had fewer tabs and categories and rather collect privacy and data collection in one location." - Participant #18

Some of the participants wished that Facebook had a search option to make it easier to locate settings, which was an option on Google. Others also complained that Facebook required too many steps to locate the right settings.

Other suggestions included using less difficult wordings and shorter explanations. Additionally, some wished that the categories were more intuitive as well as make the options less hidden.

5.3.4 The User Interface

Table 5.4: Summary of comments the participants made on the user interface.

There were too many menus
There was too much text
The site did not have a coherent style in their settings

All of the comments on the UI were for Facebook and Google. A summary can be found in Table 5.4. The main issue the participants had with the Facebook interface was its abundance of menus. As mentioned previously, many felt like there were too many categories and that the categories did not necessarily make sense.

"The words on the menu Facebook had on the left-hand side did not make sense and did not necessarily say a lot about what was inside it. I feel like they should have structured it better." - Participant #19

Additionally, many complained that the options for turning off cookies contained too much text, making it difficult to understand exactly what you were turning off.

"In Facebook's cookies, there was a bible for each of the buttons, instead of them saying exactly what it does. In addition, they try to package it in how important it is for functionality. I do not know if it is true or not, but I do not trust it." - Participant #17

Another complaint on Facebook was on the different styles different pages had, as some have a more modern feel than others.

"Suddenly you feel that you are on a journey back in time and that you are on Facebook in 2010. So it is difficult to know if you are on the right path." - Participant #20

Two participants noted that they liked the Facebook menu because it was easier to go through everything and turn everything off.

For Google many complained that there was too much text, and difficult to find the settings. Others felt like they were easy to manage because they had less text than Facebook.

One thing which the participants mentioned and which in their opinion made Google easier to use was that the settings were more or less collected in one location.

"You could do more in "my profile" [on Google]. There were not as many things you had to click through." - Participant #4

5.3.5 Familiarity with the Settings

Many of the settings were more or less new to the participants. Most of them had used the settings related to restricting profile visibility on Facebook. A few said that they had gone through their settings to turn everything off, while most had never edited any settings relating to data collection or targeted advertising.

"I think I've been to Google's pages, but have never done anything there. In addition, I think I have done it so that only friends can see what I publish on Facebook. Nothing more than that." - Participant #18

5.3.6 Relationship with Online Privacy

Table 5.5: Summary of the participants' relationship with online privacy

They care but do not know what to do
They are uncertain if what they do is enough
They feel like they have it under control
They do not really care
It does not feel like it matters what they do

The participants had many different ways of looking at their own privacy. See Table 5.5 for a summary of the answers given. Some felt like they had given it little thought, while most had some thoughts on what they should or should not share online. Many felt like they did not do enough to protect their privacy.

"Probably not good enough, considering what I study. I should probably care more about my data than I do." - Participant #12

Many reported that they did not care that much about data collection, but more about what information other people could find about them. Some of these said that they simply had not given it a lot of thought, while others did not care at all.

"I have never thought about what Facebook gives or takes from third parties, I have been more worried about who can see posts on my profile than what information Facebook has." - Participant #12

Even though they studied information security, it did not necessarily make them more worried about privacy issues.

"I don't really care. I know it is supposed to be important. I am studying security, but I don't care. Just use my data." - Participant #14

Some were generally pessimistic about whether or not their efforts made any difference.

"I'm a little pessimistic about it. Their business model is to have information so then they try to use it as much as they can." - Participant #16

5.3.7 Thoughts on Advertising and Data Collection

Table 5.6: Summary of the participants' thoughts on advertising and data collection

They feel like it is much easier to allow than to decline requests for permission
They feel like targeted ads can be scary
They like targeted advertising and customised content
They do not really care
Other people scare them more than companies

Even though they were not directly asked about it, some of the participants spoke about their experience with data collection and targeted advertising. The summary of the thoughts on targeted advertising are in Table 5.6.

Some of the participants noted how much easier it was to allow the collection of information, rather than stopping websites to track them.

"it does not seem so advanced when you say yes [to cookies], but if you try to remove them, you have to go through a lot of settings." - Participant #10

Others had also thought about the fact that some of the ads they had gotten on their page were scarily accurate, but that it had not made them change their settings.

"Sometimes, I have discussions about an ad that is very targeted advertising, and then you think «shit they must have a lot of information about me [...] ». I know they are tracking me, but I do not do anything about it." - Participant #12

One participant also expressed that he felt he had to trust the entities who were collecting information.

"In a way, you have to trust the people Google chooses to sell [your data] to." - Participant #1

Another was willing to sacrifice his privacy in order to have free services.

"I feel like I personally would have sacrificed my privacy to have these services, to some degree. It's free for a reason" - Participant #16

Quite a few participants expressed that they had only ever changed the settings for who could access their information but had not thought to do it for data collection or targeted advertising. When asked about this, multiple people found this to be much scarier.

"I think it's scarier if a person stalks me [online] than a company that wants to sell something, because then I'm just one out of many." - Participant #13

A few of the male interviewees claimed that targeted advertising did not really affect them, either because they used Adblock or because they did not look at it.

"I may get some advertising that is targeted to me, but then I really just think it's a little annoying and then I close it." - Participant #17

Lastly, one participant noted that he did not think general categories of interests were that harmful, but rather that there was a problem if they used very specific information about him for the targeting.

"I don't really care if I look at a pair of shoes and it appears on an ad, but if they are like "we know that you are gay, therefore you get this ad", then I think it is a little worse." - Participant #16

Table 5.7: Summary of the participants' privacy management strategies

They select only necessary cookies
They disable cookies when they do not wish to be tracked
They limit permissions to a minimum
They use privacy focused services
They turn off location permissions

5.3.8 Strategies in Online Privacy Management

The participants were asked what strategies they used to manage their privacy. Most of the participants had some thoughts on the subject, mostly about the choices they make often. A summary of the strategies can be found in Table 5.7.

The majority of the participants said that they chose "only necessary cookies" if it was an option, but that they rarely made an effort to manage their settings.

"Sometimes I select "only necessary" cookies if it is an alternative. But if the choice is between accepting or going in and changing the ones you want to opt-out of, then it requires a larger effort." - Participant #12

Others said that they always chose the option of "accept all" when it came to cookies.

"I accept all cookies, usually. I can not be bothered to read, I feel there is too much text." - Participant #18

For some, it mattered more what they were doing on the websites. For one of the participants, it was especially important when he was going to spend money and did not want to receive higher prices.

"I try to disable cookies for any flight reservation because they track if you have looked before to raise the prices. Every time I have to spend money I turn off cookies and look for coupon codes." - Participant #14

One of the participants was focused on always giving as little permission as he could.

"I give them as little permission as possible if there is a choice. But it's not very often I go in to the settings to change it." - Participant #1

One of the participants said that she would rather use services such as Duckduckgo in order to protect her privacy rather than edit settings.

"As a slightly neutral search engine, I use Duckduckgo, so it is my standard browser on mobile. So I'd rather go in and download it than go in and clear all the information on safari and google." - Participant #10

Another participant had made an effort on many areas, such as disabling third party cookies, using Adblock and being vary of what privacy settings he had enabled.

"I have turned off third-party cookies. I know I should use a VPN, but I do not. I have tried to deactivate everything on Facebook, but I should go in and check how it is now. I also use Adblock." - Participant #7

Quite a few of the participants noted *incognito mode* as a strategy to better their privacy, even though it did not necessarily seem like they knew what the benefits of doing so was.

"When surfing in general I use incognito, but I don't think it helps with cookies. It doesn't store any settings you've done while browsing. I guess not really anything else." - Participant #11

For some, limiting the permission of location and tracking was the most important aspect, as it seemed the most unpleasant to lose control over.

"I do not let apps track me when I do not use them and I do not let apps use my location unless it is for example [a weather app] or [an app for public transport]." - Participant #2

One of the participants in particular was conscious of what information he shared with whom.

"I am more careful the more sensitive the information is. You can say that there is a start-up barrier to giving out information. If it's a website

that seems semi-interesting but requires me to log in right away, then the value of logging in is less than my curiosity. So then I would rather not use it, than give them lots of information and email addresses. It's the same if there is more sensitive data such as social security number, then I do not bother. " - Participant #20

Others did not really feel like they had any strategies when it came to online privacy management.

"I would not really say that [that I have any strategies]. I skim the first few sentences of privacy policies and then I get bored. I approve cookies way too often" - Participant #9

5.3.9 What Keeps Them from Protecting their Privacy?

Table 5.8: Summary of the hurdles the participants face for better privacy protection

They do not notice the consequences
It does not feel like it helps
It is too difficult
They feel they may be too gullible
They find it inconvenient

A summary of the hurdles participants face can be found in Table 5.8. First, a few noted that it was difficult to spend a lot of effort protecting something they did not notice the effects of.

"It must feel like I'm actually protecting something, and that it is not work for something that is not really worth it. A bit like with the climate crisis, you have to experience it to care." - Participant #20

One of the participants felt like it did not matter what she did.

"I actually thought it was a "lost case". I have reckoned that it is not possible to do anything about it. And that what you do is little that it does not matter." - Participant #3

Others felt like it was too difficult, and that they were afraid of doing something wrong.

"It is probably because the first thing you encounter is that it is difficult and that you feel a lot of adversity. I feel I need to sit down and have time for someone to help me click the right things." - Participant #10

Some also expressed that it was more difficult that you had to actively opt-out of sharing information so that they had to actively make a choice to say no.

"I guess that it is more an "opt-out" if you don't want it instead of an "opt-in" if you do want it. I guess it would be easier if it was the other way around. But here you have to look for something and disable it, instead of actively enabling it." - Participant #11

A few also noted that they were too naive, gullible, or lazy, and therefore did not do more.

"I'm probably too gullible. I have not thought much about it and I probably do not know enough about it" - Participant #13

One of the participants had tried to turn off all cookies and settings but felt like it made his online experience much worse.

"Actually, I had turned everything off, but then my browser did not remember anything so I had to enter all websites manually, and that was annoying." - Participant #16

5.3.10 What They Wish Existed

Table 5.9: Summary of things the participants wished existed

A universal button/platform for all their privacy settings
Uniformity in setting across different platforms
Fewer settings in general
More transparency

There were different categories of things they wished existed, most of these were related to user-friendliness and transparency. A summary of this can be found in Table 5.9.

Quite a few participants wanted fewer buttons to push. One of the most common complaints with the tasks had been that it was difficult to know whether or not they had completed the task, or if they had forgotten something.

Some wanted a universal button to keep them from having to change settings for every platform.

"A universal button. That there were fewer things to press. So that you did not have to do it again if you use another browser or change to mobile or tablet." - Participant #15

Another participant wanted the browser to have a setting, so that all the choices were in one place.

"I think there could be a setting in the browser, instead of a setting on each site." - Participant #6

A third suggestion was to have one platform for regulating privacy and give users more transparency.

"It would have been nice if all such sites had had a common platform for regulating privacy and advertising, so it is possible to see all that the different ones have on you." - Participant #8

There was also a wish for more uniform design and user interfaces so that they did not have to learn all the different platform settings.

"I wish all pages had a standard, and that everyone had to follow it. This makes it difficult for each site to have its own way of doing things." - Participant #18

A few of the participants wanted to know more about what information was collected on them and wished for more transparency on what the companies knew about them.

"I would love to have more lists like Google, about who they think I am. I would like to know who I am according to the various websites." - Participant #2

One of the participants also wished for a subscription option, which gave him access to all the services without having to give away personal information.

"If Google had come to me and said that they had a subscription solution, where I could pay NOK 50 a month so that they would not collect data about me and I still had access to all the services, then I think I would have done it." - Participant #7

Chapter 6

Discussion

The studies provided valuable insights into how users might approach online privacy and what aspects should be improved. By combining and triangulating the findings from the quantitative data collected from the online survey with the qualitative data from the user experiment and interviews, it becomes more apparent what truly matters to users when it comes to privacy and privacy management. This research has also exposed some potential differences between various groups of people. This chapter is divided into three parts, answering each of the research questions introduced in Section 1.1 and discussing the findings in the light of the related work and further implications.

6.1 RQ1: What Relationship do Users Have to Their Online Privacy and Privacy Management?

It is evident that most people care about their privacy based on the results of the studies. From the questions on privacy in the online survey (Figure 5.11), most reported that they cared about what happened to their data but that they did not know how their information was being used, and found it challenging to manage their privacy. Additionally, the respondents reported that they were afraid of how their data is used and exploited, suggesting that people are worried about their online privacy. This indicates a gap between *desired privacy* and the privacy users *actually* feel they are able to achieve. About half of the respondents reported taking active measures to manage their privacy; however, half of the respondents also reported that they rarely change their default privacy settings. This might suggest that many do not know how to achieve the desired levels of privacy.

Half of the respondents in the online survey reported that they felt powerless in managing their privacy, which also was a recurring theme in the interviews. While some felt like they had control over their privacy, most reported that they did not feel like they did enough, either because they did not want to or because they did

not know how to. Most of the participants in the user experiment were young, highly educated people with at least some technical competence. Thus, it would be reasonable to assume that this group would have a more significant possibility of reaching their privacy goals than a more diverse group of participants would have. However, many of them reported that they did not do enough to protect their privacy and felt like their efforts did not matter, suggesting they suffer from *privacy fatigue* (Section 2.2.1). This might suggest a resignation among users, having become accustomed to large amounts of data collected over time. This aligns with the psychological findings from Section 2.2.1, discussing how people are good at adapting to constant or gradually increasing risks [ALB20]. Some of the interview subjects also reported that they did not dare to change settings if they were uncertain of what they were doing, as they were either afraid of losing functionality or afraid of making a mistake. This often led to them not changing default settings, which plays into the concept of *constructed preference* discussed in Section 2.2.1, where users stick to default settings because they are uncertain of what their preferences should be.

In general, the participants were divided in their thoughts on targeted advertising. The results from the online survey (Figure 5.10) showed that about half of the respondents found targeted advertising distracting. Additionally, about the same amount of people found targeted advertising useful as the number of people who did not find it helpful. From the interviews, there was also an observable division. While some found targeted content convenient, others were frustrated with how difficult it was to opt-out of data collection for targeted advertising. It also seemed like many felt that targeted advertising was the price for enjoying services on the Internet and that it was a price they were willing to pay. However, many people were scared by targeted advertising, with a majority in the online survey reporting this and several interview participants saying the same. This might stem from a feeling of not being in control of their personal information, which might be explained by the concerns respondents had about how their data is used and might be exploited.

The section on knowledge and password preferences showed that most respondents had some knowledge of basic online privacy and security concepts. Most of the respondents knew the purpose of a privacy policy. Additionally, the correct responses had the largest amount of answers to the question of storing session data. This shows that most respondents are somewhat familiar with correlated concepts. As for the password preferences, most respondents chose either the arguably strongest or second strongest passwords, which shows an overall grasp of security online. However there were some concepts which seemed more confusing. First is the question on the "Do Not Track" request, which over half the respondents answered incorrectly. The reason for this might lie in the confusing nature of this privacy feature and a lack of familiarity with this among the users. In the interviews, many of the participants mentioned that they disallowed tracking between apps when given a

choice as a privacy strategy, suggesting that the purpose of this mechanism has not been adequately explained to the general population. The other concept many seemed to struggle with was the purpose of third party cookies, even though this might be the privacy concept they have to deal with the most. This suggests that giving users more options might not better privacy literacy due to *consent fatigue* (Section 2.2.1).

The studies also revealed some gender differences when it came to online privacy relationship. While the findings need to be further validated on a larger scale and cannot be generalized for the whole population without any disclaimer, with regards to gender, the online survey suggested that women are more likely to be affected by targeted advertising, as they reported being more likely to click on an ad than their male counterparts. Additionally, they reported being scared of targeted advertising to a much greater extent. This might show how being more inclined to click on the advertisements also makes them feel less in control of their information, making it scarier. It might also be a possibility that the fact that women click more on advertisements also makes the advertisements more accurate to their specific interests, as they train the system to learn their preferences. A difference between men and women in the online survey was that men reported being more inclined to change their default privacy settings. In contrast, women reported feeling more powerless in their privacy management. This suggests that men might be better at taking a proactive approach to their data privacy management, while women might feel like they are not able to remedy the situation to the same degree.

ICT background was also a factor in privacy relationship. The respondents with an ICT background were more concerned with what happened to their data. This might be because they have more extensive knowledge of the data collection process than their non-ICT counterparts. They were also more likely to choose the most challenging password as their preferred password. This might be linked to the finding that they were also more likely to have password managers, which automatically assign such passwords. This also suggests that increased knowledge influences choices related to privacy and security online. Interestingly, they were less likely to read privacy policies and more likely to find privacy management difficult. As previously mentioned, one reason for this might be a sense of resignation. Another explanation might be that the ICT respondents might know more about the process of protecting their information and know that it is more complicated than the non-ICT participants think it is. This part was reflected in the interviews, as many of the ICT participants reported either that they did not do enough to manage their data, did not care, or doubted that their increased effort would make a difference.

Age and Education level were also factors used to find significant differences between the participants. Among other things, the older age groups were more

likely to read privacy policies than the younger age groups. However, the younger respondents (under 35) were more likely to know the purpose of a privacy policy than the older participants, suggesting a higher knowledge of privacy-related concepts in this group. This is rather interesting as it would indicate that many of those reading through privacy policies might not understand what they are reading. The age group "24-34" also reported having avoided signing up for services because of their privacy policies more than the youngest respondents. This might indicate that the youngest respondents might not find the consequences of data disclosure as considerable as the older respondents do. In general, education level did not have a significant effect on the responses in the online survey. A reason for this might be that there was not a great amount of diversity in education level among the respondents, as I suspect many of those reporting having no degree or a bachelor's degree are still studying for higher education, based on the significant amount of young respondents. However, it did show that respondents with a master's degree or higher were significantly less likely to find targeted advertising useful. This might be caused by a general skepticism in the group of more highly educated respondents.

Going back to the hypothesis that users do not think much about privacy because it is difficult to notice, mentioned in Section 1.1, seems to be partially correct. Although users might actively think about their privacy, the feeling of resignation might explain why many feel like their efforts do not matter. The explanation for why this is might be complex, but one part of the equation probably does stem from the lack of tangible consequences and *present bias*, a sense of *privacy fatigue*, as well as the human ability to adapt to constant risks, both discussed in Section 2.2.1. A summary of how users felt about their privacy can be found in Figure 6.1.

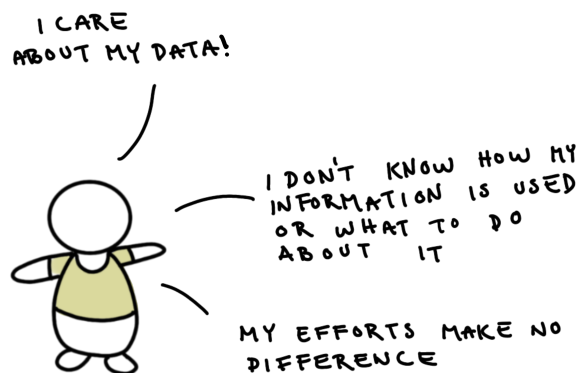


Figure 6.1: Summary the relationship users have to privacy and privacy management.

6.1.1 Issues to Privacy Management and Possible Solutions

There were multiple hurdles mentioned in the interviews and survey that might explain *why* users do not take better care of their data. First of all, there seems to be a lack of knowledge around the use and consequences, which causes indifference to the situation. This aligns with the *information asymmetry* and *bounded rationality* mentioned in Section 2.2.1, with one of the interview participants noting that he was "*probably too gullible*". By not knowing why their actions matter, it might not feel like they are actually protecting something or making an actual difference in their lives. Another major part of the issue for many participants was how difficult and inconvenient it felt. From the survey, it was evident that the most significant issues the respondents had with using privacy-focused services was it being too difficult to manage and not user-friendly enough. In the interviews, many felt like they could not edit the settings they wanted to, thus making them feel incapable of making the changes. This was primarily due to the fact that the UI was challenging to navigate and had too much text to read through. Combined with little knowledge, this might result in a lack of power of action, causing users to stick to the default settings.

The participants had some suggestions which might make their privacy management easier. A suggestion made was to have a universal system for privacy settings, either by having one joint platform for all sites or a more standardized form of setting interface. Doing this might make the process of updating privacy preferences more accessible for the general user. Additionally, many felt more transparency of what happens to their data might make their experience of dealing with privacy easier, as it would make what they are protecting more tangible. These solutions could positively affect the general willingness to increase privacy online and might even create an increased focus on what privacy issues users should care about.

6.2 RQ2: Which Strategies do Users Use to Control How Their Personal Data is Shared and Used

The users had different levels of cautiousness for different types of information. In the online survey, most reported they were mindful of what they shared on SNSs. This was also shown in the interviews, as multiple people said the only privacy management they had done was to limit who could access their Facebook profile. Many of these were more concerned with the information they shared with other people than they were with the information shared with companies or third parties. This might suggest that this is an area of privacy management that is tangible and feels easier to have a conscious relationship with, relating to the psychological factors discussed in Section 2.2.1. For instance, it is easier to grasp that the consequences of sharing a credit card number results in a loss of tangible money than what information about shopping habits could result in. From the section in the online survey about what information

they would be willing to share with advertisers, there was a clear preference for protecting sensitive information. Sensitive Personally Identifiable Information (PII), such as credit card number, social security number, address, and phone number, were among the items the respondents were least interested in sharing with advertisers. This suggests that there is a strategy among users to be mindful of what kinds of information they share online. This was also mentioned in the interviews, as one of the participants said he was unwilling to create accounts on websites unless it felt necessary. In this way, he had more control over who had access to his email, for instance.

Other strategies for managing privacy include the use of privacy-focused services. For one, most of participants used 2FA and VPN services. A reason why this might be could be explained by the increased focus on security in companies. Businesses can use these services to ensure better authentication while simultaneously allowing employees to work remotely, which has been important under the COVID-19 pandemic. AdBlock and password managers were also services respondents reported using in both the survey and the interviews. An explanation for why these services are widely used is that they better user experience by either eliminating a problem (i.e. having to remember many passwords) or making it easier to find content without distractions. A reason why a service such as Signal is not widely used or heard of might be because of the network effects mentioned in Section 2.2.4, as is the nature of messaging services. There is little incentive to switch to a more privacy friendly messaging services if there is no one to talk to on these services.

Overall, the strategies for managing online privacy seem to be contingent upon ease of use and whether or not they felt like their efforts made a difference. For instance, most of the interview participants reported accepting "only necessary" cookies if it was an available option. At the same time, they would never "edit settings" as it required too much effort. This suggests that users weigh the cost of doing something with the effort it takes for them to do it, and when it comes to privacy management, the cost has to be minimal. One of the interview subjects also noted that he turned off cookies and used incognito when he was spending money, indicating that tangible money was the threshold he needed for the cost of privacy management to be worth the effort. Additionally, multiple interview subjects noted that they limited location services when they were not required, suggesting that this information, in particular, might feel sensitive to many users. In general, it seems as though the strategies used to manage privacy require little effort, have easily available options, and involve information that is important enough to protect.

The strategies the participants reported using varied between the groups. For instance, the gender differences found in the privacy relationship also propagate into the strategies used to manage privacy. In general, men in the online survey were more

likely to use privacy-focused services than women. This reflects the above-mentioned findings, with women being less likely to report taking active measures to manage their privacy. The participants with an ICT background stood out when it came to online management strategies. For one, these participants were more likely to use VPN, encryption services, password managers, and 2FA. This makes sense, as these services are arguably more technical security solutions. This suggests that such services are easier to actively use if the user has some prior knowledge of how they work and why they might be necessary.

The hypothesis for Research Question 2 (Section 1.1), stating that users do not have many conscious privacy management strategies and default settings, does not entirely match with the results from the studies. Although many people leave default settings as they are, almost everyone has some conscious strategies regarding the information they share. For instance, with the protection of sensitive PII. However, it seems like it is easier to have a conscious response to risks when a response is prompted, than it is to actively manage privacy everywhere all the time. Overall, the most important factors for users when it comes to privacy management strategies is to see the benefits of the strategies they are using. Figure 6.2 shows a summary of what is important for users in privacy management strategies.

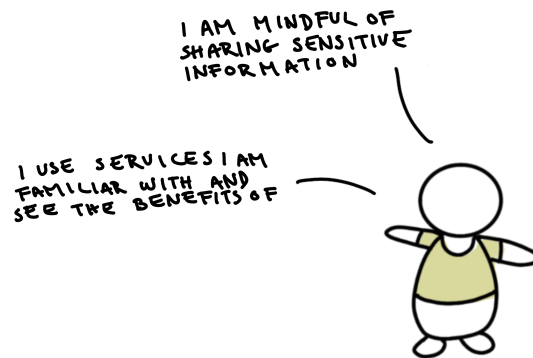


Figure 6.2: Summary of the strategies users have with privacy management.

6.3 RQ3: To What Extent do Users Perceive the Privacy Settings of Different Services as Manageable?

In general, the participants were able to complete 66% of the tasks they were given. This suggests that the participants, on average, would not be able to complete 1 out of 3 potential tasks relating to the management of settings. From Figure 5.16, it is easy to see that there are significant differences in how well a participant was

able to complete the tasks they were given. This suggests that there are significant differences in how different people intuitively would navigate through settings menus in order to reach their goals. Although some tasks seem to be more difficult than others (i.e Task 4), it seems the participants struggled with different kinds of tasks. This suggests that the issues are not with the tasks themselves but rather in how one must navigate to reach the desired setting. From the user evaluation, Task 8 was the easiest to locate and had the most usable UI, suggesting this was the task most participants were the most comfortable solving.

Combining the results from the user experiment with the interview answers, it makes sense why Facebook had the perceived most difficult settings. Even though the task most of the participants completed (Task 1) was on Facebook, this was also the task with the most confusion as to whether or not they had actually completed. This is also seen in the answers the participants gave for time spent to find the setting, where this task is clearly the most time-consuming (Figure 5.30). A reason for this might be because this task required the participants to edit multiple settings, which made them doubt whether they had found the correct setting. The most difficult task was Task 4, which was completed by 8 out of 20 participants. One of the reasons why this task was so difficult to find by many was that it was rather hidden, as can be seen in Section 4.2.4. The only possible way to edit this setting was by going through the ad settings, which many participants found rather difficult. Additionally, the Facebook settings had many different designs for different settings which might have made the process more confusing. This was a recurring theme with many of the participants in the post-task interviews.

In general, Google was seen as the second most challenging website. While most found it easy to turn off location, many struggled with finding the ad settings. One reason for this might be confusion in how the settings were organized, as they were vastly different from the settings on Facebook. Another reason might be that some of the participants went through "privacy" instead of "manage account". This page is more of an information page, with links to relevant pages. Most of the participants who went through this path felt that it was difficult with too much text. A plus many noted was the search function Google had, which helped them navigate to the correct settings. This was a feature many said they wished existed in the Facebook settings.

The most significant issues with VG and Chrome had to do with locating the settings. These tasks were largely successful once the participants found where the settings were. In VG, there was some confusion between "my preferences" and the account management through Schibsted. Additionally, the menu for personal preferences might not have been as visible due to the fact that it is a newspaper without much of a need to edit the profile. For Google Chrome, most of the issues lay

in the fact that many tried to find the settings by managing the Google profile. One interesting observation was that the correct steps for editing the browser settings were available through the search option in Google; however, none of the participants who did search managed to find the right option. This might suggest that some users have trouble reading instructions with a lot of text, which makes sense when combined with the interviews complaining about the amount of text in different settings.

There were some notable differences between the different groups' abilities to manage the privacy settings. In the user experiment, women were less likely to complete the tasks correctly. There were especially two tasks in which the women did considerably worse than the men, namely Task 4 and Task 7. The reason for this might be explained by women having less previous experience with editing such settings, as discussed in Section 6.2. For Task 7, it was, for instance, an advantage to have edited browser settings previously, which would be a plausible starting point for the individuals who had experience editing their privacy settings. The ICT participants were more likely to have correct responses for most of the tasks, suggesting that they were slightly better at solving the tasks. However, percentage-wise, they did considerably worse on Task 1 and Task 6.

6.3.1 Self-Evaluation vs Reality

After each task, the participants were asked to assess whether or not they completed the task correctly. The results of this showed significant differences in the participants' abilities to evaluate themselves on their privacy management. The results from the study showed that the participants were unable to correctly assess if they were able to complete a task for 40% of the tasks (Figure 5.23). This suggests that many users might not be aware of what privacy settings they, in reality, have on their accounts. Perhaps the most worrying category is the "incorrect yes" category (marked in yellow), in which the participants *think* they have completed a task correctly while they, in reality, have not. This would suggest that users might have privacy features enabled that they believe are turned off. Considering the psychological effects of *granular control* (Section 2.2.1), this might cause users to share more information than they otherwise would, while also not having the privacy protection they think they have.

There were differences between the categories of responses for each of the tasks (Figure 5.24). Task 2 through Task 5 all had many "incorrect yes" answers. This might suggest that these tasks were among the most difficult to find the correct setting option and that multiple similar settings made it confusing. Task 2 and Task 8 had the least amount of uncertainty. This might be because these tasks were among the easiest to know were done correctly. For Task 2, the participants were explicitly asked to turn off the use of "education" and "relationship status". At the same time,

Task 8 required the participants to turn off targeted advertising, which was also straightforward once the setting was located. Overall, there were few "incorrect no" responses (marked in purple), suggesting that most users might be more inclined to overestimate their abilities to manage their privacy, rather than under-estimate themselves.

Gender differences and ICT background had an impact on self-evaluation. With regards to gender, the men were better at knowing when they had the correct answer, which makes sense as they were also the ones with the most correct answers. On the other hand, women were more likely to have the "correct no" and "incorrect no" responses. This suggests that women might be more reserved in their self-assessments. The ICT students had a majority of the "correct yes" and "correct no" responses, suggesting that they might be better at evaluating their efforts than their non-ICT counterparts. Both groups had the same level of uncertainty.

The results of the user experiment match rather well with the hypothesis that managing privacy settings was challenging, from Section 1.1. As is evident from the results, it is rather difficult to manage privacy settings and to know whether or not it is done correctly. Overall, there was a discrepancy between how well the participants thought they were at completing the tasks, and how they in reality did. For one, the amount of *incorrect yes* responses indicate that users over estimate their abilities to make the changes they desire online. Figure 6.3 summarizes how the users perceived the management of privacy settings.

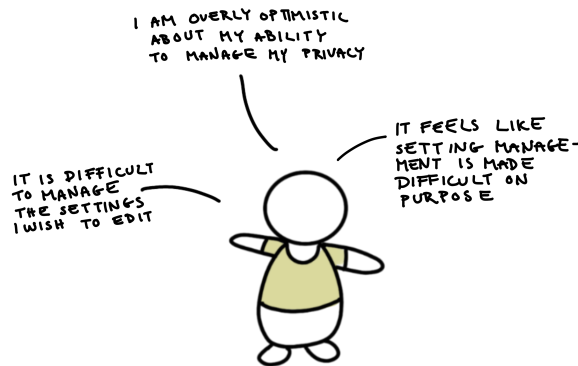


Figure 6.3: Summary of how setting management was for the users.

The difficulty in locating settings might imply that the companies do not want all settings to be easily found. Facebook had, for one, many settings which were perceived as difficult to manage. In particular, it is notable that only 40% of the participants were able to locate the ad settings for Task 4. In order to reach this page,

the participants had to go through three menus to locate the right one. Especially considering that many of those who did reach the ad preferences (which was mainly a blank page), did not realize that they had to click to get ad settings as well. This might indicate that Facebook has an incentive to hide settings related to targeted advertising, as it is the main source of their income. In Google's ad settings was that, even though the participants had the possibility to delete elements from the list used to give them targeted advertisements, this element would still return after it was deleted, which for instance happened if they tried to delete their location from this menu. Difficult language and large amounts of text were also a big source of confusion which made it difficult for many to understand what they were doing. In total, these types of choices from prominent data collectors might highlight how the availability of data is more important than giving users the option to get their desired levels of privacy.

6.4 Limitations

Some general limitations of both the online survey and the user experiment/interview is a lack of diverse representation. Although all groups were represented in the online survey, there was a clear over-representation of young, educated people as most respondents were from my network. The age group "35-44" is all very highly educated and might not accurately represent their age group. In the user experiment/interviews, all the respondents were in their 20s, and most were university students from my personal network. The selection of participants for the user experiment/interviews was equally divided between men and women and represented both ICT and non-ICT students. This allowed for some tendencies to be seen in the different groups. This also made sense, as it was groups of people I had reliable data for from the online survey. However, there were still only 20 participants, and the answers they gave might not accurately represent their groups, as small differences can still sway the results.

The structure of the online survey and user experiment also had room for improvement. For one, the survey could have tests to make sure that respondents gave consistent responses. However, there was no incentive to complete the survey other than helping a student with their thesis, making it less likely people answered in a hurry without thinking through their answers. No respondents spent less than 4 minutes on completing the survey, indicating that they were paying attention while answering. For the user experiment, it might have been more accurate to have randomization of the tasks, so that there was no learning effect making some tasks seem easier than they are. However, this would have been rather time-consuming, creating a more difficult grading process afterward.

Additionally, there is a possibility that some of the participants in the survey and

interview might have exaggerated their interest in privacy and their own personal efforts. One of the issues with self-reporting in such studies is the fact that respondents tend to respond in a way that sets them in a good light [RM16]. This might have resulted in more heavily privacy-focused responses than they would have been in reality. One example of this might be the information they were willing to share with advertisers (Figure 5.15), where a majority were unwilling to share their location, even though this is probably something many of them agree to daily because of location-based advertising. Additionally, the privacy paradox discussed in Section 2.2.3 might influence the answers given by the participants of the user experiment and online survey. With this, the participants might say that they wish to have better control over their privacy, while this might not reflect in their actions. Thus, taking the self-reported actions and desires with a grain of salt is important, as these might not match what the users do in reality. A mitigation for this limitation is the use of the user experiment, which includes also behavioral and objective measures as a reliable source for how good they are at managing privacy.t

Chapter 7

Conclusion and Future Work

It is difficult to manage online privacy. The incentives for collecting large amounts of data are considerable, with a great value being placed on personalizing content and advertisements. Because of this, many online platforms go to great lengths to optimize their user data by increasing the number of users, the time spent on their platforms, as well as the data they collect itself. This process is hidden and difficult to grasp from the user's perspective. Additionally, the process of making more privacy-focused choices can appear rather time-consuming without necessarily giving enormous noticeable benefits to the end-user. Given this context, how do users manage their privacy, and what could improve the system?

From the observations made in this thesis, there were some tendencies regarding how online privacy is for the individual. Although people care, there seems to be a feeling of powerlessness which might create a split between the privacy users wish to have and the privacy they, in reality, are able to achieve. The reason for this is complex, but a reason might be that making privacy changes is perceived as difficult because of incomprehensible settings and the use of services that might be difficult to understand and require too much effort. Additionally, it might feel like the changes have to be made in too many places, causing inaction to be more desirable. Separate groups of people also have different prerequisites to achieve the goals they might set themselves, based on knowledge and previous experience. From the user experiment, it was evident that it is difficult for users to actually complete all of the tasks they set out to do. Additionally, it is interesting to see that it can be difficult for users to assess their own efforts. This raises questions about how accessible privacy management in reality is.

The incentives to use data collection for the purposes of targeted advertising give the users little choice with regard to their privacy. A lack of transparency causes average users to have little control over where their data is collected, stored, and processed and who exactly has access to this information. There is a lot of power in profiling and targeting users for financial or political gain; however, it seems as

though the importance of this has been hushed down to ordinary people. A solution to this problem could be to better the overall privacy literacy among Internet users and ease the process of making proactive decisions regarding privacy. Regulatory action could be made to give a greater incentive to make setting management more uniform and understandable. Additionally, the platforms should have an incentive to provide users with a more active choice regarding their privacy, rather than making default settings that mainly serve their own goals. Although there probably is not one solution to the issues at hand, the combination of multiple factors would make online privacy more manageable.

From this research, we now know that users do care about their privacy, even though they might not be able to make the privacy choices they wish to make or perhaps know what they should be doing. How users perceive privacy has a significant impact on how they proceed in their online privacy management. The strategies users use to manage their privacy are contingent upon seeing the benefits of making the effort needed, either because of knowledge, ease of use, or familiarity with the potential services. Most commonly, users try to be careful with the information they share and use services they are familiar with. The biggest hurdles for using such services are a lack of user-friendliness and how difficult they are to manage. Lastly, managing privacy settings is rather difficult for the average user. Many privacy settings are hidden because they are difficult to locate or have too much text and confusing language. Making privacy more accessible to regular users would allow them to actively choose how and by whom their data is used and for what purposes it is used.

7.1 Future Work

Future work should focus on having larger participant samples to get more accurate results for multiple groups of people. For the user experiment, it would be interesting to have tested different prompts focusing on more sites and functionality. Additionally, there may be interesting differences in how manageable privacy settings are on mobile apps. It would also be interesting to see how different age groups are able to manage settings, as it might be reasonable to assume that younger individuals who have grown up with the technology in question might have an advantage in locating the settings they wish to. Different education levels might also impact these results, which might also give interesting findings.

Another interesting aspect that should be researched in future work is categorizing people based on their privacy attitudes. The results from this study indicate that different people have different strategies for managing privacy and what they find important. Thus, it would be reasonable to assume that there might not be a "one size fits all" regarding privacy. By focusing on different types of people in privacy management, using both subjective and objective measures, it might be easier to make privacy more accessible for all types of users. This research might be beneficial for lawmakers when they consider privacy legislation.

References

- [22a] *Norway's Top Websites Ranking in January 2022 | Similarweb*, Jan. 2022. [Online]. Available: <https://www.similarweb.com/top-websites/norway/>.
- [22b] *Random Name Generator - Behind the Name*, 2022. [Online]. Available: <https://www.behindthename.com/random/>.
- [22c] *This Person Does Not Exist - Random Face Generator*, 2022. [Online]. Available: <https://this-person-does-not-exist.com/en>.
- [ALB20] A. Acquisti, G. Loewenstein, and L. Brandimarte, «Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age», *Journal of Consumer Psychology*, vol. 30, no. 4, pp. 733–735, Oct. 2020.
- [Alp22] Alphabet Inc., «Alphabet Announces Fourth Quarter and Fiscal Year 2021 Results MOUNTAIN VIEW, Calif», Tech. Rep., 2022.
- [ATW16] A. Acquisti, C. Taylor, and L. Wagman, *The Economics of Privacy*, Jun. 2016.
- [Bar06] S. B. Barnes, «A privacy paradox: Social networking in the United States», *First Monday*, vol. 11, no. 9, Sep. 2006. [Online]. Available: <https://doi.org/10.5210/fm.v11i9.1394>.
- [BCW21] K. Birch, D. T. Cochrane, and C. Ward, «Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech», *Big Data and Society*, vol. 8, no. 1, 2021.
- [BdJ17] S. Barth and M. D. de Jong, *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*, Nov. 2017.
- [Bha18] P. Bhatia, *GDPR summary: Overview of 10 key requirements*, Jan. 2018. [Online]. Available: <https://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/>.
- [BN18] V. Benndorf and H. T. Normann, «The Willingness to Sell Personal Data», *Scandinavian Journal of Economics*, vol. 120, no. 4, pp. 1260–1278, Oct. 2018.
- [CC15] H. T. Chen and W. Chen, «Couldn't or wouldn't? the influence of privacy concerns and self-efficacy in privacy management on privacy protection», *Cyberpsychology, Behavior, and Social Networking*, vol. 18, no. 1, pp. 13–19, Jan. 2015.

- [CG18] C. Cadwalladr and E. Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, 2018. [Online]. Available: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- [CPJ18] H. Choi, J. Park, and Y. Jung, «The role of privacy fatigue in online privacy behavior», *Computers in Human Behavior*, vol. 81, pp. 42–51, Apr. 2018.
- [Cre09] J. W. Creswell, *Research Design*, 3rd ed. Sage, 2009.
- [Dal06] E. Dal Bó, *Regulatory capture: A review*, Jun. 2006.
- [Dat20] Datatilsynet, «Personvernundersøkelsen 2019-2020», 2020.
- [DN18] M. Degeling and J. Nierhoff, «Tracking and tricking a profiler», in *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, Oct. 2018, pp. 1–13.
- [DT15] T. Dienlin and S. Trepte, «Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors», *European Journal of Social Psychology*, vol. 45, no. 3, pp. 285–297, Apr. 2015.
- [Edw18] L. Edwards, «Data Protection : Enter the General Data Protection Regulation», Tech. Rep., 2018. [Online]. Available: <https://ssrn.com/abstract=3182454>.
- [EN16] S. Englehardt and A. Narayanan, «Online tracking: A 1-million-site measurement and analysis», in *Proceedings of the ACM Conference on Computer and Communications Security*, vol. 24-28-October-2016, Association for Computing Machinery, Oct. 2016, pp. 1388–1401.
- [Eur16] European Commission, *Regulation (EU) 2016/679 of the European Parliament and of the Council*, 2016.
- [FB12] A. Farahat and M. Bailey, «How Effective is Targeted Advertising?», in *WWW 2012 – Session: Advertising on the Web 1*, ACM, 2012, p. 1078.
- [FH21] G. A. Fowler and T. Hunter, *iPhone apps can track you even after you tell them not to - The Washington Post*, 2021. [Online]. Available: <https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/>.
- [Fie17] A. Field, *Discovering Statistics Using IBM SPSS Statistics*, 5th ed. SAGE Publications Ltd, 2017.
- [GB21] S. Garg and N. Baliyan, *Comparative analysis of Android and iOS from security viewpoint*, May 2021.
- [GE21] M. Graham and J. Elias, *How does Google make money?*, May 2021. [Online]. Available: <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html>.
- [Gle22] A. Glenn, *Zuckerberg threatens to 'shut down' Facebook and Instagram across Europe*, Feb. 2022. [Online]. Available: <https://www.euroweeklynews.com/2022/02/07/zuckerberg-threatens-to-shut-down-facebook-and-instagram-across-europe/>.

- [Hor22] V. M. Horvei, *Tinder-priser varierer med flere hundre kroner i måneden - Tek.no*, 2022. [Online]. Available: <https://www.tek.no/nyheter/nyhet/i/eEvayl/tinder-priser-varierer-med-flere-hundre-kroner-i-maaneden>.
- [ILRB21] D. Ibdah, N. Lachtar, *et al.*, «Why Should i Read the Privacy Policy, i Just Need the Service’: A Study on Attitudes and Perceptions Toward Privacy Policies», *IEEE Access*, vol. 9, pp. 166 465–166 487, 2021.
- [KMBP18] A. Karaj, S. Macbeth, *et al.*, «WhoTracks .Me: Shedding light on the opaque world of online tracking», Apr. 2018. [Online]. Available: <http://arxiv.org/abs/1804.08959>.
- [Kri01] D. M. Kristol, «HTTP Cookies: Standards, Privacy, and Politics», *ACM Transactions on Internet Technology*, vol. 1, no. 2, pp. 151–198, 2001.
- [LC20] H. Lee and C. H. Cho, «Digital advertising: present and future prospects», *International Journal of Advertising*, vol. 39, no. 3, pp. 332–341, Apr. 2020.
- [Les22] K. Leswing, *Facebook says Apple iOS privacy change will cost \$10 billion this year*, 2022. [Online]. Available: <https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html>.
- [LH21] J. Lin and S. Halloran, *Study: Effectiveness of Apple’s App Tracking Transparency / Transparency Matters*, Sep. 2021. [Online]. Available: <https://blog.lockdownprivacy.com/2021/09/22/study-effectiveness-of-apples-app-tracking-transparency.html>.
- [LUW+13] P. G. Leon, B. Ur, *et al.*, «What Matters to Users? Factors that Affect Users’ Willingness to Share Information with Online Advertisers», Tech. Rep., 2013. [Online]. Available: <https://www.mturk.com>.
- [Met22] Meta, «Meta Reports Fourth Quarter and Full Year 2021 Results», Tech. Rep., 2022.
- [MHF19] N. Momen, M. Hatamian, and L. Fritsch, «Did App Privacy Improve after the GDPR?», *IEEE Security and Privacy*, vol. 17, no. 6, pp. 10–20, Nov. 2019.
- [Min21] Miniwatts Marketing Group, *World Internet Users Statistics and 2021 World Population Stats*, 2021. [Online]. Available: <https://www.internetworldstats.com/stats.htm>.
- [NC20] J. Nadler and D. N. Cicilline, «Investigation of Competition in Digital Markets», pp. 1–450, 2020.
- [NKJ+13] N. Nikiforakis, A. Kapravelos, *et al.*, «Cookieless monster: Exploring the ecosystem of web-based device fingerprinting», in *Proceedings - IEEE Symposium on Security and Privacy*, 2013, pp. 541–555.
- [NSK22] M. Namara, H. Sloan, and B. P. Knijnenburg, «The Effectiveness of Adaptation Methods in Improving User Engagement and Privacy Protection on Social Network Sites», *Proceedings on Privacy Enhancing Technologies*, vol. 2022, no. 1, pp. 629–648, Jan. 2022.

- [OO20] J. A. Obar and A. Oeldorf-Hirsch, «The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services», *Information, Communication & Society*, vol. 23, no. 1, pp. 128–147, 2020. [Online]. Available: <https://www.tandfonline.com/action/journalInformation?journalCode=rics20>.
- [PI21] PwC and Iab, «Internet Advertising Revenue Report», Tech. Rep., 2021.
- [PW18] J. Plesch and I. Wolff, «Personal-data disclosure in a field experiment: Evidence on explicit prices, political attitudes, and privacy preferences», *Games*, vol. 9, no. 2, Jun. 2018.
- [RM16] C. Robson and McCartanm Kieran, *Real World Research*, 4th ed. Wiley, 2016, pp. 241–306.
- [RTKvE18] L. Royakkers, J. Timmer, *et al.*, «Societal and ethical issues of digitization», *Ethics and Information Technology*, vol. 20, no. 2, pp. 127–142, Jun. 2018.
- [SAP+17] R. Sen, S. Ahmad, *et al.*, «Inside the Walled Garden: Deconstructing Facebook’s Free Basics Program», *Computer Communication Review*, vol. 47, no. 5, 2017.
- [SD09] J. Sauro and J. S. Dumas, «Comparison of Three One-Question, Post-Task Usability Questionnaires», in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM Press, 2009, pp. 1599–1608.
- [ST17] J. E. Short and S. Todd, «What’s Your Data Worth?», *MIT Sloan Management Review*, vol. 58, no. 3, 2017. [Online]. Available: <http://mitsmr.com/2mUheim>.
- [Sta21] A. Stanley, *Apple’s Privacy Policy Cost Snap, Facebook, Twitter, and YouTube an Estimated \$9.85 Billion in Revenue*, 2021. [Online]. Available: <https://gizmodo.com/apples-privacy-policy-cost-snap-facebook-twitter-and-1847971994>.
- [Sta22] Statcounter, *Browser Market Share Worldwide*, 2022. [Online]. Available: <https://gs.statcounter.com/>.
- [TSLB21] J. Tang, H. Shoemaker, *et al.*, «Defining Privacy: How Users Interpret Technical Terms in Privacy Policies», *Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. 3, pp. 70–94, Jul. 2021.
- [Tuc14] C. E. Tucker, «Social networks, personalized advertising, and privacy controls», *Journal of Marketing Research*, vol. 51, no. 5, pp. 546–562, Oct. 2014.
- [UTD+20] T. Urban, D. Tatang, *et al.*, «Measuring the Impact of the GDPR on Data Sharing in Ad Networks», in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2020*, Association for Computing Machinery, Inc, Oct. 2020, pp. 222–235.
- [Zub19] S. Zuboff, *The Age of Surveillance Capitalism*. Profile Books, 2019.
- [ØA21] H. Øverby and J. A. Audestad, «The Digital Economy», in *Introduction to Digital Economics*, Springer, 2021, pp. 1–15.

- [AAB+17] A. Acquisti, I. Adjerid, *et al.*, «Nudges for privacy and security: Understanding and assisting users' choices online», *ACM Computing Surveys*, vol. 50, no. 3, Aug. 2017.

Appendix

Online Survey



Online Privacy Management

Page 1

Mandatory fields are marked with a star *

This survey is part of a master's thesis in Communication Technology at The Norwegian University of Science and Technology (NTNU). Its goal is to map online privacy attitudes among Internet users. The data is collected completely anonymously, and can not be connected to you. The survey takes about 10 minutes to complete.

Open questions can be answered in both English or Norwegian.

If you live in the Trondheim area and could be interested in participating in a user experiment related to this topic (and receive a gift card in return for your time), please contact me at ikvassil@stud.ntnu.no.

 Page break

Page 2

Mandatory fields are marked with a star *

First of all, we ask you a number of questions about you.

Which gender do you identify with? *

- Female
- Male
- Non-binary
- Prefer not to say

How old are you? *

- Under 18
- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- Over 64

Which nationality do you have? *

- Norwegian
- Other European country
- Non-European country

What is your highest completed education level? *

- None
- Some high school
- High school
- Bachelor's degree or equivalent
- Master's degree or higher


Do you have or are you studying for a degree in computer science, communication technology, information security or related field? *

- Yes
- No

Now we will ask you a couple of questions related to your preferences and understanding of privacy and security-related concepts.

Imagine you would create an account for a new digital service right now, which type of password from the examples below would you prefer to use? *

- football
- 1234567890
- acidanthera
- aa123456@
- jbdkfdjll34904@*Ed4G2+
- I don't know

 Page break

114 A. ONLINE SURVEY

the following questions based on your current knowledge and understanding (please do not use Google or similar). If a term sounds unfamiliar, you can just indicate this.

In your understanding, which of the descriptions below best describe the purpose of a privacy policy? *

- It explains how your data will be protected
- It is a legal document that says how users' data will be collected and used
- It explains how the company keeps confidential the information it collects on users
- It says that the company will not share users data with other sites or companies without permission
- I don't know

In your understanding, if you send a "Do Not Track request", are websites or apps able to track you? *

With tracking we refer to monitoring of your web-surfing behavior (e.g., which websites you visit).

- Yes
- No
- I don't know

In your understanding, when you are using a so-called "private browsing" window or "incognito mode" while surfing the internet, where is data from your browsing session stored? *

Multiple answers can be correct.

- On your machine or device
- On machines or servers belonging to the websites browsed
- On the machines or servers belonging to third parties
- On the machines or servers belonging to third parties
- Nowhere
- I don't know

In your understanding, what does it mean if a website uses third party cookies? (if you don't know, please just write that). *

Mandatory fields are marked with a star *

Now, we will ask you a couple of questions related to "targeted advertising". Please indicate to which extent you agree or disagree with the statements below.

With targeted advertising, we refer to a type of online advertising that is targeting certain groups of users e.g., because of their interests, preferences, previous browsing behavior.

	Strongly dis- agree	Disagree	Neutral	Agree	Strongly agree
In general, I find targeted advertising useful *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In general, I find targeted advertising distracting *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In general, I find targeted advertising to be relevant to my interests *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I usually don't look at the ads that appear on the websites I visit *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Targeted advertising is necessary to enjoy free services on the Internet *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have clicked on an ad in order to get more information about the product *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am more likely to click on targeted ads on my phone than on my computer *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sometimes, targeted advertising scares me *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

 Page break

Mandatory fields are marked with a star *

116 A. ONLINE SURVEY

We are also interested in your opinions and typical practices related to data privacy. To which extent do you agree or disagree with the statements below?

Data privacy or information privacy refers to the privacy linked to your own personal data.

	Strongly dis- agree	Disagree	Neutral	Agree	Strongly agree
I am concerned that the information I submit to online vendors can be misused *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I take active measures to manage my privacy *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am mindful of the information I share on social media *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am afraid someone might exploit the information I have shared online *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I rarely change default privacy settings *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am worried about my data being leaked *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel powerless in managing my privacy *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am tired of dealing with privacy issues *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I doubt my efforts to protect my data contribute to anything *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I don't care what happens to my data *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I always read privacy policies before accepting them *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I know how the information I shared is being used *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have avoided signing up for a service because I was worried about their privacy policies *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I find it easy to manage my privacy online *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I have trouble finding the privacy settings I wish to edit *



 Page break

Page 6

Mandatory fields are marked with a star *

Which of the services listed below have you already heard of? *

Several answers are possible.

- VPN services
- Duckduckgo
- Signal
- Tor browser
- Encryption services
- Adblock
- Password managers
- Two-Factor Authentication
- None of the above

118 A. ONLINE SURVEY

How often do you use the services listed below?

	Daily basis	Weekly basis	Monthly basis	Never
VPN services *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Duckduckgo *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Signal *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tor browser *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Encryption services *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Adblock *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Password managers *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Two-Factor Authentication *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Are there any other services that you currently use or previously have used to protect your own (online) privacy? *

- Yes
- No
- I don't know

In case you use, or have previously used, any additional services for this purpose, please list them here.

- This element is only shown when the option "Yes" is selected in the question "Are there any other services that you currently use or previously have used to protect your own (online) privacy?"

The biggest hurdles for using privacy-focused services is...


"Privacy-focused services" refers to services that help protect your online privacy in some way. I.e the services listed above.

	Strongly dis- agree	Disagree	Neutral	Agree	Strongly agree	Not applica- ble
It's too expensive *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It's not user friendly enough *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None of my friends use it *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It's too difficult to manage *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Are there any other barriers or hurdles which keep you from using privacy-focused services like the examples mentioned above? *

- Yes
- No
- I don't know

Which barriers/hurdles keep you from using privacy-focused services? Please explain in your own words.

-  This element is only shown when the option "Yes" is selected in the question "Are there any other barriers or hurdles which keep you from using privacy-focused services like the examples mentioned above?"

 Page break

Mandatory fields are marked with a star *

In the next part, we will ask you a couple of questions about your information sharing practices.

120 A. ONLINE SURVEY

Would you be willing to share the following types of information with an advertising network?

"Advertising network", in this context, refers to a company that collects information about users in order to create a profile on a person. If a shop wants to advertise directly to people with certain characteristics (e.g age, location), the advertising network can use this information to show the advert to the relevant people.

	Yes	No	It depends
Which operating system you use *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your location *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your name *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your email address *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your phone number *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your address *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your credit card number *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your social security number (fødselsnummer) *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your age *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your income bracket *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your gender *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your religion *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your sexual orientation *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

If you answered "it depends" on the questions above, what does it depend on? Please explain in your own words.

Mandatory fields are marked with a star *

[See recent changes in Nettskjje](#)

Do you have any additional comments on your online privacy management or on this study?

If you live in the Trondheim area and want to participate in further studies (and receive a gift card), contact me at ikvassil@stud.ntnu.no

Appendix **B**
User Experiment

Lab study

Side 1

Obligatoriske felter er merket med stjerne *

Before the assignment begins:

Participant number *

 Sideskift

Side 2

Obligatoriske felter er merket med stjerne *

Information about the assignment

You will now be asked to complete some tasks on a test computer. All users are already logged in, so there is no **need to use your own profile information**. This is not a test of your skills, but rather of the system. If you get stuck on a task, move on to the next task.

The tasks will be given to you one by one. **Do not go to the next task** before you are finished with the task you are on (Either if you complete or give up). There are no "trick tasks".

After each task, you will be asked to fill out a questionnaire.

Good luck!

 Sideskift

Side 3

Obligatoriske felter er merket med stjerne *

Facebook - 1

Imagine you want to limit the information that is collected about you online. Your over all goal is that companies can not share your information with third parties, such as advertising companies.

Your first thought is that you want to limit the information from social media, because you know it is a place with personal information. Therefore you go to *Facebook* to change your settings.

Your first goal is to limit who is able to see your profile.

 Sideskift

Side 4

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

Questions about the task.

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

 Sideskift

Side 5

Obligatoriske felter er merket med stjerne *

Facebook - 2

Your second goal is to limit the information which is used to give you targeted advertising. You do not want your relationship status or education to be used to give you advertisements.

 Sideskift

Side 6

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

Questions about the task.

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Side 7

Obligatoriske felter er merket med stjerne *

Facebook - 3

You want to make it so Facebook cannot track what you do on other websites.



Side 8

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

Questions about the task.

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

 Sideskift

Side 9

Obligatoriske felter er merket med stjerne *

Facebook - 4

You do not want Facebook to use your information advertise outside of Facebook.

 Sideskift

Side 10

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

Questions about the task.

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Side 11

Obligatoriske felter er merket med stjerne *

Google - 1

You remember that Google also has a network of information. Therefore you go to Google to manage your settings.

First, you want to get an overview of the information Google uses to give you targeted advertising.



Side 12

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

Questions about the task.

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Side 13

Obligatoriske felter er merket med stjerne *

Google - 2

You don't want your position to be used to give you any suggestions.



Side 14

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

130 B. USER EXPERIMENT

Questions about the task.

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Side 15

Obligatoriske felter er merket med stjerne *

Google Chrome

You want your web browser "Google Chrome" not to allow third party cookies.



Side 16

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

Questions about the task.

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Side 17

Obligatoriske felter er merket med stjerne *

VG - 1

You remember that you often get ads on vg.no (Norway's biggest online newspaper), related to things you have previously searched for. You want to turn off targeted advertisement here.



Side 18

Obligatoriske felter er merket med stjerne *

Remember to close the tab!

Did you complete the task? *

- Yes
- No
- Uncertain

132 B. USER EXPERIMENT

Questions about the task.

[Se nylige endringer i Nettskje](#)

	Totally dis- agree	Disagree	Neutral	Agree	Totally agree
The setting was easy to locate. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The user interface (how the page looks) was easy to use. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am happy with the amount of time I used to complete the task. *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

 Sideskift

Side 19

Obligatoriske felter er merket med stjerne *

Thank you for your participation!

Appendix **C**
Interview Guide

Interview Guide

Session length: ~ 1 hour

(Recording begins after the execution of tasks)

1. Introduction

- Introduction on the subject
- Information on the consent form
- Explain the project

2. In general

- Age, occupation, field of study

3. Execution of tasks

- [The interviewee is asked to navigate around web pages to solve various tasks, see assignment text below]

4. Questions about the tasks

- How do you think it went?
- Are you familiar with the pages you visited?
 - Do you use them often?
- Have you used these settings before?
 - Why / why not
- Was there anything that surprised you?
- What did you find most difficult?
- Were any of the settings you found more difficult than others?
- Is there anything that could have made it easier?

5. Questions about own habits

- What is your relationship to online privacy?
 - Do they have any thoughts about it
 - Do they take an active or passive role?
- What kind of strategies would you say you have for managing privacy online?
 - If they cannot think of something:
 - Do you often change your privacy settings?
 - Read the privacy statements before accepting
 - Do you change the default cookies?
- What are your biggest barriers to protect your privacy?
- Is there anything you are missing in your privacy management?

6. Closing

- Anything else you want to add?
- Thank you for participating
- Tell that all data is deleted after it has been transcribed
- Give gift cards

