Cookies, cookies everywhere!

A qualitative interview study about how internet users interact with cookie consent notices

Cookies, cookies överallt!
En kvalitativ intervjustudie om hur internetanvändare interagerar med samtyckesrutor

Niklas Hofstad
Anton Lundqvist

The faculty for humanities and social sciences

Media and Communication

Bachelor's thesis 15 hp

Michael Karlsson

2021-06-04

Abstract

The purpose of this study is to examine what reasons internet users have for accepting, declining, or adjusting cookie settings. The study's research question is: *what reasons do Internet users have for accepting, declining, or adjusting cookie settings?* To answer the research question, we constructed three research support questions: 1) *how do internet users access the internet?*, 2) *What are internet users' perspectives on privacy on the internet?, 3) How do internet users interact with cookie consent notices?*

The study's theoretical framework consists of informed consent, contextual integrity, nudging, and political economy. We conducted semi-structured interviews in order to get a deeper understanding of the internet users' experiences with cookie consent notices. We analyzed the material through thematic coding. Due to the Covid19 pandemic, all interviews were conducted through Zoom. The sample consisted of eight media and communication students at Karlstad University.

There were four key findings: 1) The interviewees in our study accessed the internet primarily via applications on their smartphones. 2) There were mixed opinions about who has the greatest responsibility for private citizens' privacy on the internet. Although many thought that the individual bears most of the responsibility, a majority thought there is a need for more governmental regulation regarding collecting and processing private data. 3) All interviewees thought cookie consent notices are an excellent tool for protecting one's privacy, but none of them adjusted the cookie settings regularly when prompted by cookie consent notices. 4) The reasons why the interviewees accept cookies without adjusting cookie settings varied. Habits and annoyance were key factors.

The current climate where notice and choice is the de facto privacy measure for internet users is not sustainable. In conclusion, legislators and policymakers should focus on regulating how personal data is processed rather than pushing the responsibility of safeguarding personal data onto the users.

Keywords: Cookie, Consent, GDPR, Informed, Personal data, Privacy,

Sammanfattning

Syftet med denna studie är att undersöka vilka skäl internetanvändare har för att acceptera, neka eller justera cookie-inställningar. Studien undersöker forskningsfrågan: *Vilka skäl har internetanvändare för att acceptera, neka, eller justera cookie-inställningar?* För att besvara forskningsfrågan konstruerade vi tre stödfrågor: *1) Hur får internetanvändare tillgång till internet? 2) Vad är är internetanvändarnas perspektiv gällande integritet på internet? 3) Hur interagerar internetanvändare med samtyckesrutor?*

Studiens teoretiska referensram bestod av informerat samtycke, kontextuell integritet, nudging, och politisk ekonomi. För att få reda på vilka skäl internetanvändare har för acceptera, neka, eller justera samtyckesrutor genomfördes åtta stycken semistrukturerade intervjuer. Intervjumaterialet analyserades genom tematisk kodning. På grund av Covid19-pandemin valde vi att genomföra intervjuerna via Zoom. Urvalet bestod av åtta medie- och kommunikationsvetenskapsstudenter på Karlstads universitet.

Analysen gav fyra huvudresultat: 1)Intervjupersonerna surfar främst på internet genom smartphone-applikationer. 2) Det var blandade åsikter om vem som har störst ansvar för privatpersoners integritet på internet. En del menade att individen har störst ansvar, men en majoritet tyckte att det behövs mer statlig reglering angående hur personuppgifter på internet hanteras. 3) Alla intervjupersonerna tyckte att samtyckesrutor är utmärkta verktyg för privatpersoner att skydda sina personuppgifter. Själv justerar de däremot inte cookie-inställningarna på en daglig basis när de interagerar med samtyckesrutor. 4) Skälen till varför intervjupersonerna godkänner cookies utan att justera cookie-inställningarna varierar. Huvudskälen var vana och irritation.

Det nuvarande situationen där "noitce and choice" är grundpelaren för integritet på internet är inte hållbar. Vår slutsats är att lagstiftare och beslutsfattare borde fokusera på ökad regulering av hur personuppgifter processeras, istället för att flytta ansvaret för ens integritet på privatpersoner.

Nyckelord: Cookie, Consent, GDPR, Informed, Personal data, Privacy.

Acknowledgments

Both authors, Niklas Hofstad and Anton Lundqvist, have taken equal responsibility for planning and writing the thesis.

We want to express our deepest gratitude to Didem Özkul, our supervisor. Her feedback and guidance were invaluable. We want to extend our thanks to the interviewees; without you, the thesis would not have been possible. We also want to thank our girlfriends for their love and support.

Karlstad June 4, 2021

Niklas Hofstad & Anton Lundqvist

Table of content

1. Introduction

Imagine walking to a mall. At the entrance, an almost square-shaped security guard stands tall with a clipboard. He asks you to read and accept the mall's terms of services before you enter. You, who just want window-shop, quickly glance at the clipboard and accept the terms of services. All of a sudden, three people come out of nowhere. The security guard notices how startled you got and assures you that they only take notes to improve the mall's user experience. Inside the mall, the three people start following you, taking notes about where you look, how many steps you have walked, and what clothes you are wearing.

After a while, you notice that most advertisements inside the mall are deals on espresso. You think, 'Hmmm, peculiar. I've been craving an espresso for a while now.', without realizing that you have paid more attention to coffee-related products than other items in the past 20 minutes. Your note-taking friends, however, knew exactly how many minutes your gaze was fixed on various cafeteria logos, coffee presses, and coffee cups.

You decide to have an espresso at your favorite mall cafeteria. The barista asks you to read and accept the cafeterias' terms of condition before ordering the espresso. You quickly answer 'yes' to the terms of service. After all, you want the coffee A.S.A.P. Four more people appear before the purchase is finalized. Parts of your new entourage begin chatting with each other, exchanging notes about you. Some of them seem to work at the same company.

This little thought experiment demonstrates, in straightforward terms, how personal information is collected and analyzed on the internet to sell advertisements.

1.1 Background and problem description

The quest for personal data on the internet can be likened to the new gold rush. Generally speaking, governments and government agencies, researchers, technology companies, online retailers, and content creators want access to personal data (Andrejevic, 2014; Kennedy, 2016; Nissenbaum, 2010; van Dijck, 2014). Personal data is, according to the General Data Protection Regulation (GDPR.):

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person ((EU) 2016/679, p. 33)

There are a plethora of reasons why personal data is sought after by the actors mentioned above. For example, governments and government agencies have always handled personal data, like healthcare data and tax registers. However, personal data generated on the internet allows for, e.g., continuous monitoring of and access to criminal networks (Hare, 2016), understanding the human condition in an online context (Kennedy, 2016), and personalized advertisement.

Personal data is easily generated on the internet, and the majority of Swedes generate personal data on the internet everyday (Andersson et al., 2020; Internetstiftelsen, 2019). Every action made by a user can be logged by trackers and thereafter analyzed for otherwise unattainable or hidden knowledge through data mining (Acar et al., 2014; Coenen, 2011; Libert, 2015, 2018).Trackers, also known as third-party cookies, are spawned on ca. 60 percent of the top one million websites (Alexa ranking[1]) according to data from 2015 (Libert, 2015). Google has by far the most trackers present on the web, tracking users on ca. 80 percent of the top one million websites (Alexa Ranking).

The collection and processing of personal data remain a controversial topic. Privacy scholars have criticized the methods employed by actors, especially technology companies, to collect, store, and use personal data (Hu & Sastry, 2020; Kennedy, 2016; Nissenbaum, 2010; van Dijck, 2014). The National Security Agency (NSA.) scandal of 2013 and the Cambridge Analytica scandal of 2018 confirmed what privacy scholars had warned politicians and legislators about for decades. The Snowden leaks revealed how the NSA. had access to major tech companies' databases containing non-anonymized personal data used for global surveillance operations (Black, 2013). Five years later, the Cambridge Analytica scandal exposed how a small network of actors, legally (though debated), got hold of Facebook profiles and processed them in an attempt to manipulate swing voters into voting for Donald Trump in the 2016 U.S. presidential election (Cadwalladr & Graham-Harrison, 2018).Perhaps as controversial as the deliberate attempt to manipulate millions of voters: the users consented to the data collection when they signed up for their Facebook accounts.

When users visit websites or sign up for online accounts, they must, according to EU legislation before (European Data Protection Supervisor, n.d.; Lee, 2011) and after the implementation of the GDPR ((EU) 2016/679), give the websites their informed consent to process personal data. The idea is built on Westin's (1967) theories about privacy, which stresses the importance of notice and choice. This can be accomplished with dialogue windows encouraging users to read

[1] Alexa ranking is a web traffic measurement from Amazon, https://www.alexa.com/about

the website's terms of service and then requiring users to click 'I agree to the terms of service' (Obar & Oeldorf-Hirsch, 2020). However, as alluded to in the previous paragraph, does informed consent work as intended?

The research on informed consent suggests that notice and choice are ineffective because most users "agree" to websites' terms of service without reading them (Kulyk et al., 2018; Obar & Oeldorf-Hirsch, 2020; Utz et al., 2019). Yet, the GDPR, considered to be one of the most rigid privacy laws ever to have existed (Linden et al., 2019), is based on the notion of notice and choice. On the other hand, data processing actors must fulfill more criteria to comply with the GDPR than previous privacy legislation. For example, users must be offered the option to control the flow of their personal data. Currently, this is achieved with a dialogue window known as cookie consent notices, which are similar to clickwrap but with the options to enable or disable third-party cookies (Utz et al., 2019).

The usefulness of cookie consent notices, for the same reasons as with other types of informed consent on the internet, is questioned (Degeling et al., 2019; Sanchez-Rola et al., 2019; Utz et al., 2019). Still, the research on users' understanding of cookie consent notices is scarce. The GDPR treats data collection and processing as potential privacy threats to users, but do the users feel the same? Kulyk et al. (2018) suggest there is a mix of perspectives on this topic, although their sample of paid respondents is a validity issue. Besides, privacy concern does not necessarily lead to privacy behavior (Choi et al., 2018; Hargittai & Marwick, 2016; Kokolakis, 2017).

Additionally, cookie consent notices are not widely used on Android (the operating system) applications (Mehrnezhad, 2020). We have not found studies about iOS applications and cookies, though anecdotally, this applies to iOS as well. Applications like Facebook's Messenger and the Amazon shopping app do not display cookie consent messages when users use them. Nevertheless, these applications collect personal data just like regular websites.

1.2 Purpose and Research question

The purpose of this study is thus threefold. Firstly, we want to explore internet users' privacy attitudes regarding data collection and data processing. Secondly, we want to understand how they interact with cookie consent notices and the reasoning behind their actions. Thirdly, we want to evaluate if cookie consent notices are the right approach to solve the privacy problems related to collecting and processing personal data on the internet.

Our research question (RQ) is: *what reasons do Internet users have for accepting, declining, or adjusting cookie settings?*

We made three research support questions (RSQs) to answer the RQ:

RSQ1: How do internet users access the internet?

How one accesses the internet determines to a large degree if one experiences cookie consent notices or not. Accessing the internet via applications reduces the exposure of cookie consent notices dramatically (Mehrnezhad, 2020). If the majority of time spent on the internet is via applications, then the EU's efforts to give internet users more control over their private data might be in vain.

RSQ2: What are internet users' perspectives on privacy on the internet?

The literature on privacy attitudes and privacy behavior is divided. Proponents of notice and choice argue that informed users are prone to protect their personal information (Nissenbaum, 2010). In the case of our study, it would mean that privacy-minded users would adjust cookie settings when interacting with cookie consent notices. If users do not know the purpose of cookie consent notices, they have little incentive to adjust the cookie settings. Critics of notice and choice maintain that knowledge is secondary: structural power asymmetry by design is the real problem. We want to explore where internet users stand on these issues.

RSQ3: How do internet users interact with cookie consent notices?

How internet users interact with cookie consent notices varies (Kulyk et al., 2018; Utz et al., 2019). However, in-depth exploration of how internet users reason about their interaction is missing in the scientific literature.

1.3 Definitions

Big data

Big Data refers to, in short, the concept of collecting and analyzing huge amounts of data sets, which was impossible only a couple of years back (boyd & Crawford, 2012; Mayer-Schönberger & Cukier, 2013)

Data-mining

Data mining refers to the processing and extracting information from a large set of data in order to discover unattainable or hidden knowledge within datasets (Coenen, 2011).

Digital literacy

Digital literacy refers to one's ability to understand and comprehend information through various digital platforms (Park, 2013). Digital literacy is, for instance, one's understanding of using search engines, web browsers, email, etcetera.

Cookies and trackers

A website cookie, also known as an HTTPS cookie, is a small piece of data from a website stored on the user's computer when the user browses the web. Cookies have several functions. They are mainly used for session management, storing information in the shopping cart, and login information. Secondly, they are used for personalization by storing user settings, saving themes and preferences. Thirdly, cookies track the users by recording and analyzing the user's behavior (Mozilla, n.d.).

Browse-wrap

Browse-wraps are shown as a banner on the website. It then contains the information that the user accepts the terms of service by accessing the website (Gupta, 2012)

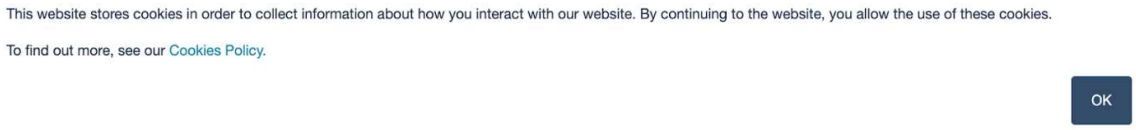

Figure 1. Example of browse-wrap. Source: https://spot.io/

Clickwrap

Clickwraps are similar to browse-wraps. However, they do often force the user to interact with it to access the website. For example, the user must confirm the terms of service by clicking on the 'I accept button' in order to use the service (Obar & Oeldorf-Hirsch, 2020)

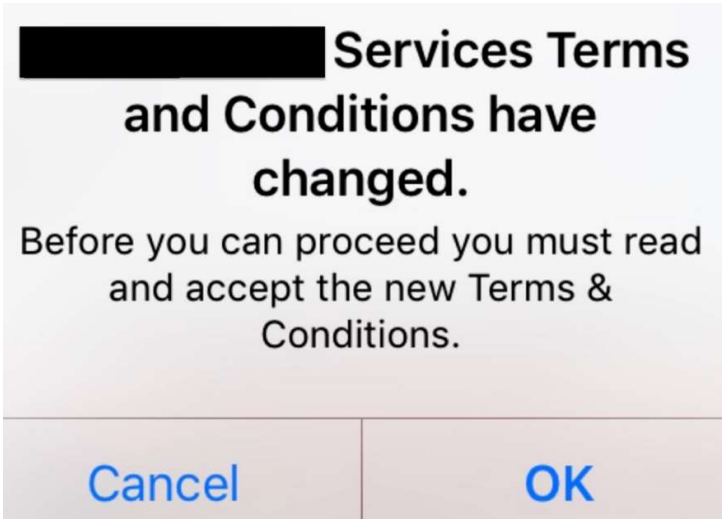

Figure 2. Example of clickwrap. Source: https://discussions.apple.com/thread/250327991

Cookie consent notice

A cookie consent notification pop-up on websites, showing the user the website's cookie policy. It allows them to accept cookies, set preferences for the use of cookies, and in rare cases, reject cookies (Utz et al., 2019).

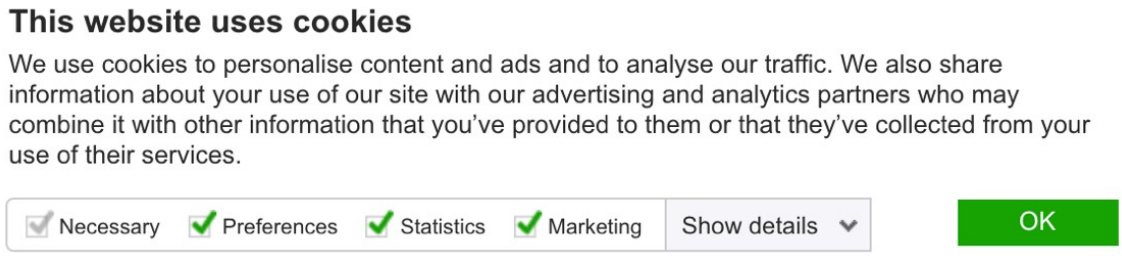

Figure 3. Example of clickwrap. Source: https://www.datadrivenu.com/gdpr-cookie-consent-google-analytics/

1.4 Limitations

Our study can be applied to every adult in Sweden. Due to the current Covid-19 situation discussed in chapter 3, we chose to limit our study to media and communication students at Karlstad University.

1.5 Outline

The first chapter, *Introduction*, presents the study's background, problem description, purpose, and research question. It also explains how we have chosen to delimit the study. The second chapter, *Literature review*, describes previous research and then continues into our study's theoretical framework. This study utilizes four theories, notice and choice, contextual integrity, nudging, and political economy.

The third chapter, *Method*, deals with our qualitative method and motivates why we have chosen to use semi-structured interviews. The fourth chapter, *Findings and analysis*, presents themes found in the interview data. We support our findings with relevant theories and studies. The fifth chapter, *Discussion and conclusion*, consists of a discussion and conclusion. In this section, we discuss the purpose of the study and ensure that the study's questions are answered. The sixth chapter, *Future Studies*, discusses the potential of using the study's findings in new contexts. The final chapter, *Implications for society*, discusses the study's findings and their implications for society.

2. Literature Review

In order to create a deeper understanding of the chapter, we have chosen to split the chapter into two parts. First, in section 2.1, we present previous research that focuses on different privacy and data concepts. Secondly, in section 2.2, we present the relevant theories to the study, which are Notice and Choice, Contextual integrity, Nudging, and Political economy.

2.1 Previous research

2.1.1 Properties of personal data

As mentioned in Chapter 1, personal data on the internet has become a valuable commodity for several actors. Advocates argue that personal data fuels innovation (Mayer-Schönberger & Cukier, 2013), keeps criminals and terrorists at bay (Hare, 2016), and improves the users' online experiences by personalizing content via sophisticated analysis of their surfing habits (Gillespie, 2014)

The GDPR's definition of personal data from a European perspective covers much ground. Additionally, Internet Protocol (IP) addresses, cookie identifiers, and other online identifiers are closely related to personal data because they can be combined with unique identifiers to create user profiles ((EU) 2016/679). For example, browsing an online store or reading an online newspaper does not necessarily generate personal data, except for IP address information. Because of the advancements in technology, the lines between personal and non-personal data are blurred. Algorithmic processing of personal data combines different datasets and can turn seemingly non-personal data into personal data (Gillespie, 2014; Mai, 2019; Nissenbaum, 2010; Solove, 2006; van Hoboken, 2019).

The processing of data is known as data mining, which refers to various techniques used for processing and extracting information from the data sets (Coenen, 2011). The ontology of data mining is that data does not need human interpretation to exist, meaning data is objective (Floridi, 2010). The epistemology of data mining says that data is manipulable: data can be controlled, owned, and measured (Mai, 2019). Obtaining and manipulating data is, according to this philosophy, a way to objectively understand nature. With enough data, combined with proper statistical analysis, one can unearth otherwise unattainable knowledge and even predict human behavior (Boyd & Crawford, 2012; Kennedy, 2016; Mayer-Schönberger & Cukier, 2013; Jose van Dijck, 2014).

The massive data sets needed for data mining are colloquially known as big data. The term refers to, in short, the accumulation and storage of large amounts of data (Mayer-Schönberger &

Cukier, 2013). On the internet, big data is generated since every action performed by a user can be translated into binary data. Actions such as liking a picture on Instagram, joining a Facebook discussion, or simply browsing the web generate quantitative data (Boyd & Crawford, 2012; Coenen, 2011; Jose van Dijck, 2014).

2.1.2 Collecting personal data

Web pages are, in most cases, not unitary objects. Their building stones often consist of a collection of media elements (Libert, 2018; Roosendaal, 2012). These media elements are integrated into complex modular systems forming intricate webs spanning across the web (van Hoboken, 2019). Website content like advertisements, social media share buttons, embedded video players, tracking pixels, and etcetera can place trackers (small pieces of code) onto users' web browsers (European Commission, 2016; Leenes & Kosta, 2015; Libert, 2015).

The ingenious aspect of trackers is the web server's ability to read trackers placed by the server regardless of which website the tracker is on, for as long as it is the same tracker (Hu & Sastry, 2020; Leenes & Kosta, 2015). Thus, a web server can keep track of internet users' behavior across numerous websites for as long as the websites use the same tracking cookie. As Hu and Sastry point out: '*TP* [third party affiliate] *that appears on both https://www.bbc.com, and https://www.nytimes.com is able to infer that a user visited both sites, and therefore can infer that the user might be someone who is interested in news and current affairs*' (Hu & Sastry, 2020, p. 76).

The internet contains a considerable number of trackers. Englehardt and Narayanan (2016) found that the average website places 17,7 third-party trackers onto its users' browsers. Websites that provide editorial content, which in many cases rely on advertisement for funding, load a higher average of third-party trackers (between 25 to 35). Furthermore, Google, Facebook, Twitter, and AdNexus are present on more than ten percent of the top one million websites (Alexa ranking). Google, which provides numerous web analytics and advertising tools, is present on ca. 80 percent of the top one million websites, according to figures from 2015 (Libert, 2015).

Online accounts also allow websites to collect personal data. The crowdfunded web service Terms of Service Didn't Read (ToS;DR) grades websites' terms of services and makes the opaque details transparent to internet users (ToS;DR, n.d.), a problem we will discuss later in detail. Several notable companies are listed on ToS;DR's homepage. Facebook, e.g., collects personal data whether one has an account or not if a website uses Facebook Products (Facebook, 2020). Google can, among a plethora of things, view: one's Chrome browser history (if it is synced to a Google account); search words; voice and audio information when one uses audio features;

purchase activity; and people with whom one has communicated or shared content with (Google, 2021). Moreover, results from a 2017 study found that Google and Facebook trackers were implemented in over 50 percent of Android (the operative system) applications (Papadopoulos et al., 2017). The dataset consisted of 116 applications based on the top 300 websites (Alexa ranking, February 2016), i.e., only 116 of the 300 websites had smartphone application counterparts.

2.1.3 Personal data and privacy

Collecting and processing personal data is a controversial topic for several reasons(e.g., Andrejevic, 2014; Kennedy, 2016; Nissenbaum, 2010; van Dijck, 2013). In this study, we will focus on the privacy aspect. Privacy scholar David Solove describes privacy as *'a concept in disarray. Nobody can articulate what it means*.' (Solove, 2008, p. 1). Additionally, he remarks that '*When people claim that privacy should be protected, it is unclear precisely what they mean*' (Solove, 2008, p. 7). He argues that *privacy* is an umbrella term referring to related yet distinct groups of things (Solove, 2006). Therefore, referring to *privacy* as a constant is not advisable since *privacy* can be understood differently depending on which context it is used. We discuss the term more in detail in section 2.2.

The NSA scandal was a milestone in the debate about privacy on the internet. The documents leaked by Edward Snowden revealed a global surveillance operation spearheaded by the U.S. government as a part of the war on terror (Black, 2013). The NSA accessed emails, chat logs, and other data from Google, Facebook, Microsoft, Apple, and five other internet companies. Sophisticated data mining programs helped analyze vast amounts of data and spy on unknowing civilians at an unprecedented scale. The collected data became 'digital dossiers' (Solovo, 2006)

A contemporary real-life example of how the processing of personal information can go wrong is China's social credit system (SCS). China has concentrated enormous resources on collecting information about its citizens from several information streams, including smartphone applications and social media (Liang et al., 2018). The collected information is processed, i.e., coded, to determine if the citizens engage in 'good' or 'bad' behavior (Engelmann et al., 2019; Liang et al., 2018). 'Good' behavior can be rewarded with material rewards or reputation gain, while 'bad' behavior can lead to exclusion from material goods or public shaming. These two categories are constructed with a particular ideology in mind (the Chinese Communist Party's). Hence, the ruling party coerces Chinese citizens to follow its ideology.

Even though SCS is exclusive to China, some voices point out that similar systems in China already exist in Western Societies (C. S. Lee, 2019; Síthigh & Siems, 2019; Wong & Dobson, 2019). Wong and Dobson write:

> Several companies have begun to experiment with social media data to build an algorithmic model that is able to measure creditworthiness through the evaluation of one's phone number, email and social media accounts. The posts, pictures and connections the individual has on their social media profiles will give companies the ability to evaluate how the individual is currently living their life in alignment or not with deemed creditworthiness, based on this representational data. (Wong & Dobson, 2019, p. 225)

The Cambridge Analytica scandal illustrates Wong and Dobson's points. Instead of creditworthiness, the Cambridge Analytica algorithm was used for identifying probable swing voters and target them with tailored pro-Trump 2016 election messages. (Cadwalladr & Graham-Harrison, 2018). It might seem implausible that over 50 million Facebook users agreed to share their Facebook information and friends list with third-party app developers. However, they actually consented to share their data and friends lists via third-party applications when they signed up for their Facebook account, which was the root of the whole scandal.

2.1.4 Informed consent

Informed consent in the context of the internet is a legally binding contract where the user agrees to a website's terms of service and privacy policies (Gupta, 2012; P. Lee, 2011). It is a form of notice and choice, which we discuss further in section 2.2.1. Before the GDPR, browse-wrap and clickwrap were the most commonly used tools to communicate terms of conditions in web-based agreements (Gupta, 2012). Browse-wrap is, in broad terms, a banner at the bottom of the website notifying the user that by browsing the website, the user agrees to the terms of service. The clickwrap serves a similar function; the key difference is the user interaction. With clickwraps, users must confirm if they agree to the terms of service by clicking on the "I accept" button. The action of clicking accept is interpreted as affirmative action and therefore legally binding.

The usefulness of browse-wrap and clickwrap is debated (Cate, 2010; Gupta, 2012; Nissenbaum, 2011; Obar & Oeldorf-Hirsch, 2020; van Eijk et al., 2012). Studies show that most users do not read websites' terms of services or privacy policies despite their well-meant intentions. The reasons 'why' vary. From the literature, we have discerned four common explanations: how policies are drafted, users' digital literacy skills, expectations, and options.

Drafting a clear yet detailed privacy policy or terms of condition policy is challenging (Gluck et al., 2016). One possible explanation could be that data controllers (legally responsible persons for

handling internet users' information) are preoccupied with complying with existing legislation rather than meeting the users' needs, interests, and preferences (Custers et al., 2014). The word count and complexity of privacy policies vary. Privacy policies for popular websites like Facebook and Google require college-level reading skills (measured with the Lexile test) to comprehend them (Litman-Navarro, 2019). On average, the length of privacy policies is 2250 words (Sanchez-Rola et al., 2019). Consequently, most internet users consent to privacy policies without reading them (Auxier et al., 2019; McDonald & Cranor, 2008; Obar & Oeldorf-Hirsch, 2020).

Besides the length and legal jargon of privacy policies, users must comprehend the technical aspects of the internet to grasp why data collection can affect users' privacy. Research on digital literacy suggests that the majority of internet users lack an understanding of surveillance practices on standard websites (Hinds et al., 2020; Park, 2013; van Eijk et al., 2012). Additionally, even knowledgeable internet users struggle with understanding the contents of privacy policies (Reidenberg et al., 2015). If internet users do not understand how and why their personal data is used, they have minimal incentive to control their personal data. However, this is not to say that all internet users lack awareness (Boerman et al., 2018; Hargittai & Marwick, 2016).

Some privacy-oriented users try to control the flow of their personal data via technical and behavioral means (Choi et al., 2018). However, it is exhausting to read every privacy policy on every website one visits, adjust every cookie setting one interacts with, and keep track of trackers with browser plugins. The steps needed to protect one's privacy can lead to privacy fatigue, resulting in cynicism and reduced privacy behavior (Choi et al., 2018; Keith et al., 2014). For example, Choi et al. (2018) discovered that the participants who scored high on privacy fatigue were more likely to do nothing in response to the misuse of their personal information.

In the context of socializing with friends, people want to have instantaneous interactions, regardless of the activities take place offline or online (Nissenbaum, 2011). Making friends read privacy policies before interacting with each other goes against their expectations of how one usually interacts in this context. The same can be said about most human behavior: interjecting privacy policies where they usually are not found becomes a nuisance. Participants in a study by Obar and Oeldorf-Hirsch (2020) aptly expressed that '*Privacy policies are too long,' There are too many privacy policies to read*' (Anonymous participant, Obar & Oeldorf-Hirsch, 2020, p. 142).

Regarding options, a vital business strategy used by the top seven technology[2] companies is acquisition (van Hoboken, 2019). Acquiring smaller companies allows the companies to grow

[2] Apple, Alphabet, Amazon, Alibaba, Facebook, Microsoft, and Tencent.

their respective platforms, which is beneficial for the companies in terms of gaining access to personal data. On the other hand, users have fewer available options. As a result, the users are dependent on companies with underwhelming care about their users' personal data for providing online services. Opting out from, e.g., social media is not an option in today's society for most people (Hargittai & Marwick, 2016; Hinds et al., 2020; Kennedy et al., 2017).

2.1.5 The GDPR and the cookie consent notice

The GDPR is a collaborative effort between EU member states to address and improve how personal information is collected and processed. Like its predecessor, Directive 95/46/EC, the GDPR's primary function is to protect individuals' fundamental rights and freedoms regarding the processing and movement of personal data (European Data Protection Supervisor, n.d.; Integritetsskydsmyndigheten, n.d.). A unique aspect of the GDPR is its attempt to keep up with the ever-evolving technological landscape. For example, the regulation addresses the issue of algorithms blurring the boundary between information and private information, specifically in the context of algorithmic profiling:

> Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. ((EU) 2016/679, p. 6).

Like previous privacy policies and legislations, the GDPR is influenced by the notion of notifying and choice. The first chapter in the GDPR states that consent must be given before websites can collect and process personal data ((EU) 2016/679, s. 6). The parties who collect personal information are responsible for informing the user about: what information they collect; the purpose of collecting it; how they process it; and any third parties who get access to it ((EU) 2016/679). Furthermore, the information must be transparent (the transparency principle), i.e., presented in '*a concise, transparent, intelligible, and easily accessible form, using clear and plain language*' ((EU) 2016/679, p. 39).

The purpose of transparency and consent is to give internet users control over the flow of their personal data. If users object to Company A sharing their personal information with Company B, then the users should have the option to adjust this or revoke their consent. According to the GDPR:

> Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data ((EU) 2016/679, p. 6).

The risk of not transparently informing users and getting their consent are fines up to 20 000 000 euros or 4 percent of the sanctioned entity's worldwide annual turnover ((EU) 2016/679, p. 83). Because of the risk of severe fines, the use of cookie consent notices has boomed since the implementation of the GDPR (Degeling et al., 2019; Kulyk et al., 2018; Utz et al., 2019). As mentioned in Chapter 1, cookie consent notices are similar to clickwrap notices and have been around since 2011 (Lee, 2011). Both notify users about privacy-related policies (cookie policies and terms of service, respectively), and both require affirmative action to be legally binding. However, the purpose of cookie consent notices is to allow users to adjust the number of non-essential cookies (e.g., trackers) websites can load onto the users' browsers.

The cookie consent designs vary and are often made by third-party companies (Degeling et al., 2019; Utz et al., 2019). To our experience, cookie consent notices generally consist of; a dialogue window; with a short text informing the user about the website's cookie policy, an 'Accept all cookies' button, and a 'Configure cookies' or 'Decline all non-essential cookies' button. Clicking the configure cookies option leads the users to a new page where the users can read about and adjust several cookie options by ticking boxes. The last aspect is crucial since it is supposed to give the users more control over the flow of their personal data.

Unfortunately, studies have listed several issues with cookie consent notices. Firstly, certain cookies are placed onto web browsers before the users even get the option to reject or accept cookies (Libert, 2015; Sanchez-Rola et al., 2019). Secondly, 51 percent of 101 available Android apps out of 116 web services do not display cookie consent notices (Mehrnezhad, 2020), despite smartphone applications collecting personal data (Papadopoulos et al., 2017). These issues are more related to regulation than how users interact with cookies, but it is important to note since it relates to their usefulness as privacy-protection tools. Secondly, we have noted that cookie consent notices sometimes load with pre-ticked boxes, meaning that users must manually untick every box if they want to adjust the flow of their personal data. This becomes tedious if websites have 30 or more third-party cookies pre-ticked. Furthermore, it is illegal according to the GDPR ((EU) 2016/679, p. 6).

Few studies have explored how users interact with cookie consent notices. Kulyk et al. (2018) conducted a paid, online qualitative survey to research users' thoughts about websites' cookie usage and how the users interacted with cookie consent notices with different designs. The results showed that the users react quite differently when exposed to cookie consent notices. A large subset was annoyed by the dialogue window; others were concerned about their privacy because they perceived the notices as threatening.

Utz et al. (2019) conducted mixed-methods field experiments to investigate the design aspects of cookie consent notices. Their sample consisted of 80 000 German internet users. The results indicated that nudging (highlighting 'Accept' buttons or pre-selecting checkboxes) significantly impacted the participants' acceptance of cookies. The same effect happened when given a binary choice (accepting or declining cookies). The vendor style (dialogue windows with multiple, fine-grained cookie options) was more successful at encouraging participants to adjust the cookie settings, suggesting that these individuals are willing to expend extra effort to decline cookies. Machuletz and Böhme (2020) got similar results in their experiment. They suggested that design elements used in consent dialogs of popular websites might nudge users to share more personal data than they are comfortable sharing.

To our knowledge, no study has explored users' broader understanding of privacy and their interaction with cookie policies. The studies about user interaction with cookie policy that we have read have been questionnaire studies or experiments.

2.2 Theories

2.2.1. Notice and choice

Arguably, one of the most common concepts of privacy is notice and choice (Nissenbaum, 2010; Solove, 2008). It is an individualistic approach that emphasizes the importance of the individual's autonomy and control over personal information. In his book, *Privacy and Freedom,* Alan Westin writes that humans seek autonomy to avoid being manipulated or dominated by others (Westin, 1967). The greatest threat to one's autonomy is '*the possibility that someone may penetrate the inner zone and learn his ultimate secrets, either by physical or psychological means*' (Westin, 1967, p. 33). From Westin and his peers' perspectives, knowledge, skills, and abilities (control) are crucial for protecting one's privacy (Masur, 2020).

Westin's view on privacy has greatly influenced scholars, lawmakers, and policy-makers (Nissenbaum, 2010). His legacy is echoed in the digital world primarily through the idea of informed consent dialogue windows. According to Westin (1967), rational individuals will take

the necessary measures to protect their privacy. In line with this logic, the primary measure users should take on the internet is to read websites' terms of service and privacy policy and judge if their privacy is at stake or not. The GDPR is noticeably influenced by Westin, e.g. since it has informed consent as a key privacy mechanism.

2.2.2 Contextual integrity

In contrast to privacy as control of personal information, contextual integrity views data as information that requires interpretation to be meaningful (Mai, 2019; Nissenbaum, 2010; Nissenbaum, 2011). Contextual integrity suggests that humans care about different things in different contexts, and there are complex norms that arise to guide our actions in each context (Nissenbaum, 2010; Nissenbaum, 2011). Nissenbaum compares and contrasts situations where personal data transaction is acceptable, even expected, with situations where personal data transaction is sensitive. For example, it is acceptable to share one's address and personal identity number with healthcare personnel, but one would not do the same when buying groceries at the local store.

Contextual integrity does not consider the internet and the physical world to be disparate from each other (Nissenbaum, 2011). For example, bank errands online or offline are not wholly different situations. In both contexts, it is customary to read contracts and agreements carefully. In contrast, no one expects to read agreements when socializing with friends and family. Yet, this is how the internet works these days. Every website is required to inform and (in Europe, due to the GDPR) get the users' consent before allowing them access to banks or social media, or any other kind of content. This constant bombardment of notifications to read privacy policies, according to Nissenbaum, goes against our expectations and causes all sorts of negative emotions.

Nissenbaum (2011) disagrees with the reliance on informed consent as the primary method to safeguard internet users' privacy. She argues that the information needed to convey data processing practices is too detailed or too simplified for ordinary internet users, a phenomenon known as the transparency paradox:

> summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference: who are the business associates and what information is being shared with them; what are their commitments; what steps are taken to anonymize information; how will that information be processed and used. (Nissenbaum, 2011, p. 63)

Proponents of contextual integrity maintain that policymakers and legislators should instead assure appropriate flows of personal data, regardless of context (Nissenbaum, 2011; Solove, 2006). Mai and van Hoboken suggest that since it is impossible to control and regulate interpretations and production meaning, the real goal for policymakers and legislators should be to regulate the situations where meaning is created (Mai, 2019; van Hoboken, 2019).

2.2.3 Nudging

Acquisti et al. (2017) and Utz et al. (2019) write about the concept of *nudging*, which is when the websites try to steer users into performing certain behaviors. In the case of cookie consent notices, nudging means steering users to accept preselected options. A typical design is when the accept button is in a more highlighted color, with preselected options to accept all cookies. Some websites nudge the user in a more privacy-friendly way, Karlstad University homepage, for example, as shown in figure 4, which highlights '*No, thanks*.' Kau.se is the only website that we have noticed that does so.

Figure 4. Screenshot of cookie consent notice from Karlstad University's homepage.
Source: https://www.kau.se/en

Nudging is also related to Privacy by Design, which is when websites direct the users' behavior toward more benign choices. Acquisti et al. (2017) explain that there are multiple factors online which make privacy and security a complex subject. Firstly, technology and the online world are constantly evolving, including the threats that technological advancements bring. Secondly, protecting one's data requires much knowledge, and the tradeoff with doing so is generally complicated. Thirdly, making decisions online requires a lot of different factors to have in mind.

In everyday life, people make decisions based on feelings, emotions, and mental shortcuts. Acquisti et al. (2017) suggest that "every design decision potentially nudges users in one direction or another." (p. 44:3). When people lack awareness of the internet, especially if they lack insight on privacy and security, the results might be unwanted. For example, user data is constantly being collected depending on every choice one makes on a website. It might lead to the individuals' data being used by third parties with bad intentions, for example hacking or data breaches. (Acquisti et al., 2017). Effective nudges are, for example, password meters, when users are shown whether their password is strong or not, which can lead to the user creating stronger passwords. While this might be true, some users might dislike the password meter and see them as irritating (Ur et al., 2012).

One of the most compelling arguments by Acquisti et al. is that nudging can be used to '*help users overcome cognitive and behavioral hurdles that may impact their privacy and security decisions*.' (Acquisti et al. 2017, p.44:33) In today's current online environment, marketers are well educated on how to take advantage of consumers' data to the fullest to sell their services. One great example of nudging is when cookie consent notices or dialog boxes pop up. The "agree" button is often brighter, while the "disagree/customize button" is less inviting to click.

Another form of nudging the user more positively is done by adapting Privacy by Design, consisting of seven principles written by Ann Cavoukian (2011). The first principle proposes that the highest authorities enforce a higher privacy standard. Secondly, Privacy by Design should automatically protect individuals. '*If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy - it is built into the system, by default*.' (Cavoukian, 2011, p. 2) The idea of Privacy by Design is more of a holistic approach embedded into the internet's architecture, which would mean that higher authorities would have to improve existing privacy designs. Privacy by Design's goal is to have privacy *and* security without choosing between privacy or security. Privacy by Design seeks to have more transparency and visibility for the companies and the end-users (Cavoukian, 2009, 2011). Most importantly, Privacy by Design should be designed with a user-friendly focus on individual users.

2.2.4 Political economy

Political economy in the context of media critically '*examines how media and communication systems and content reinforce, challenge and influence existing class and social relations*' (Jin, 2021, p. 3). Informed consent, viewed under the lens of political economy, is a tool used for sustaining the power asymmetry between website owners and users (Andrejevic, 2014; Fuchs, 2012). The fact that users are presented with two options, 1) consent or 2) stop using the service, puts the users at a disadvantage. The condensation of the web (van Hoboken, 2019) and the societal integration of internet services provided by powerful technology companies mean users have few to no options besides consenting to websites' terms of condition.

The cookie consent notices have the potential to be a game-changer. Giving users the ability to control the flow of their personal data by enabling and disabling trackers might empower users to take back control over their privacy. However, the research on the matter is sparse. Therefore, it is interesting to investigate why or why not users take the opportunity to control the flow of their personal data.

3. Method

In this chapter, we discuss the methodology of our study. It addresses the choice of method, sampling, how the data collection was executed, and how the data was analyzed. Furthermore, we discuss the study's ethics, validity, reliability, and generalizability.

3.1 Semi-structured interview

The purpose of conducting a semi-structured interview is to understand a phenomenon from the interviewees' perspective (Kvale & Brinkmann, 2014; McIntosh & Morse, 2015). Their experiences are then analyzed to find patterns, hidden meanings, and other relevant information to answer the study's research questions.

Researchers from various disciplines use semi-structured interviews as a data collection method. The purpose of conducting a semi-structured interview varies, and the research question dictates it. McIntosh & Morse (2015) lists four types of semi-structured interviews: the descriptive/confirmative: the descriptive/corrective; the descriptive/interpretive; and descriptive/divergent. Our study is of the descriptive/corrective type, meaning we are juxtaposing '*what is known about an experience … with the perspectives of those … who have actual material knowledge of this experience*' (McIntosh & Morse, 2015, p. 3).

Put into the context of our study, the GDPR encourages internet users to take control over their personal data. The phenomenon we focus on, cookie consent notices, is the most common tool for giving internet users the option to adjust cookie settings on websites. As established in our literature review, a deeper understanding of the cookie consent phenomena from the perspective of internet users is missing. Closely related topics like clickwrap and informed consent (notice and choice) suggest that internet users do not read privacy policies when prompted. Despite the similarities between clickwrap and cookie consent notices, the latter offer internet users the option of adjusting what data websites can collect. So, while informed consent might have failed in related areas, it is unclear if these past failures translate to cookie consent notices.

3.1.1 The interview guide

Semi-structured interviews are similar to a regular conversation between two parties but focus on exploring themes related to the study's research question (Kvale & Brinkmann, 2014). The interview guide helps the interviewers explore specific themes and improvise at given moments (Kvale & Brinkmann, 2014; McIntosh & Morse, 2015). These aspects of semi-structured interviews keep the conversation fluid and evolving without losing track of what one tries to explore. Comparatively, unstructured interviews are difficult because the questions are

formulated on the spot, meaning every interview is unique and puts significant demands on the interviewer. On the other hand, fully structured interviews do not allow the researcher to diverge from the interview guide. Therefore, exploring spontaneously interesting aspects of the interviewees' experiences of a phenomenon is lost.

The interview guide (Appendix 1) is organized into themes based on the research support questions (RSQs). The first theme is the *Introduction*. It functioned as an icebreaker, allowing the interviewee to get comfortable with the interview setting. The theme also aimed at getting answers to RSQ1 (*How do internet users access the internet?)*. Question 1 (*Tell us a little about yourself*), which technically is not a question, was asked as a warm-up question. Question 2 (*Approximately, how many accounts do you use regularly?*) and Question 3 (*What websites do you usually visit, except for social media?*) were asked to get a picture of the interviewees' surfing habits. The interviewees' answers were used later on in the interview to demonstrate and discuss how the interviewees' surfing patterns generate complex tracker networks, which we will come to shortly. Question 4 (*Which device do you use most frequently when you surf?*) relates to political economy. If an interviewee primarily uses social media and does so via smartphone applications, then the interviewee most likely does not get the opportunity to adjust cookie settings since applications (to our knowledge) do not display cookie consent notices.

The second theme, *Integrity on the internet*, was designed to answer RSQ2 (*What are internet users' perspectives on privacy on the internet?*). It aimed at exploring the interviewees' understanding of data collection and data processing and their perspectives on privacy. Question 5 (*What kind of information about you do you think websites collect when you visit them?*) and Question 6 (*How is the collected information used, you reckon?*) were based on research about digital literacy (Choi et al., 2020; Masur, 2020; Park, 2013).

Question 7 (*What information about you is acceptable for websites to collect?*) and Question 8 (*What information about you is unacceptable for websites to collect?*) were asked to examine the interviewees' perspectives on privacy. The questions allowed us to juxtapose contextual integrity (Nissenbaum, 2010; Nissenbaum, 2011) and Westin's (1967) notions about privacy.

Question 9 (*Do you protect your privacy on the internet, and in that case, how?*) is related to digital literacy since studies have shown that privacy-minded individuals use different techniques to protect their personal data . Question 10 (*Who do you think has the greatest responsibility for protecting private citizens' integrity on the internet?*) juxtaposes political economy with Westin's notions about privacy. Political economists argue for more regulation (Andrejevic, 2014; Fuchs, 2012; Jose van Dijck, 2014; van

Hoboken, 2019), while Westin (1967) and his peers (Nissenbaum, 2010) would argue that the system is reasonably satisfactory: it is the users who bear the greatest responsibility. However, we wanted to know what the users thought about the topic.

Additionally, the findings from the second theme were compared with the theme *cookie consent notices* to evaluate if digital literacy and privacy perspectives relate to cookie adjustment. Westin (1967) would argue that informed individuals would adjust cookies to gain control over their personal data since they are responsible for their privacy. Consequently, individuals with good digital literacy and understanding of privacy risks will protect their privacy by, e.g., adjusting cookie settings. Political economists would instead argue that there are structural problems with cookie consent notices, just like with any other kind of informed consent on the internet (Andrejevic, 2014): knowledge is not the determining factor for privacy behavior.

The third theme, *Cookie consent notices*, was designed to answer the third RSQ (*How do internet users interact with cookie consent notices?*). It aimed to explore how the interviewees interact with cookie consent notices and the reasoning behind their actions. Question 11 (*What do you usually do when you see cookie consent notices?*) and Question 12 (*Are there situations where you change the cookie setting, and in that case why?*) were based on survey questions from Utz. et al.'s study (2019). Question 13 (*Do you usually read the cookie policy when a cookie consent notice shows up?*) is based on Obar and Oeldorf-Hirsch (2020) study about clickwrap and policy reading.

Question 14 (*What do you think is positive about cookie consent notices?*) and Question 15 (*What do you think is negative about cookie consent notices*?) were based on Utz et al.'s (2019) and Degeling et al.'s studies (2019). We wanted to expand their studies and get more in-depth knowledge about how users perceive cookie consent notices. In addition, the questions also seek to discover new potentials and drawbacks of cookie consent notices, which the previous studies might have missed due to their methodological choices.

Because the design of cookie consent notices varies, meaning the interviewees probably have different perceptions of how they look, we decided to show the interviewees the same pictures of one type of cookie consent notice. Figure 5, Figure 6, and Figure 7 are from the same cookie consent notice. Figure 5 is the first view users see when entering the website allabolag.se[3]. Figure 6 is what users see when they click on '*more options*' (fler alternativ, in Swedish). Figure 7 is what users see when they click on the "arrows" next to the word '*off*' (av, in Swedish)

[3] Allabolag is a Swedish online business directory https://www.allabolag.se/om/informationen

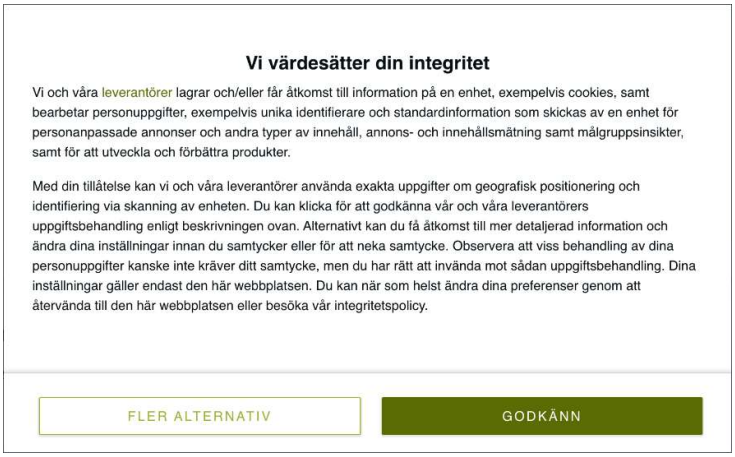

Figure 5. Screenshot of cookie consent example #1 used during the interviews. Source: https://www.allabolag.se/

Figure 6. Screenshot of cookie consent example #2 used during the interviews. Source: https://www.allabolag.se

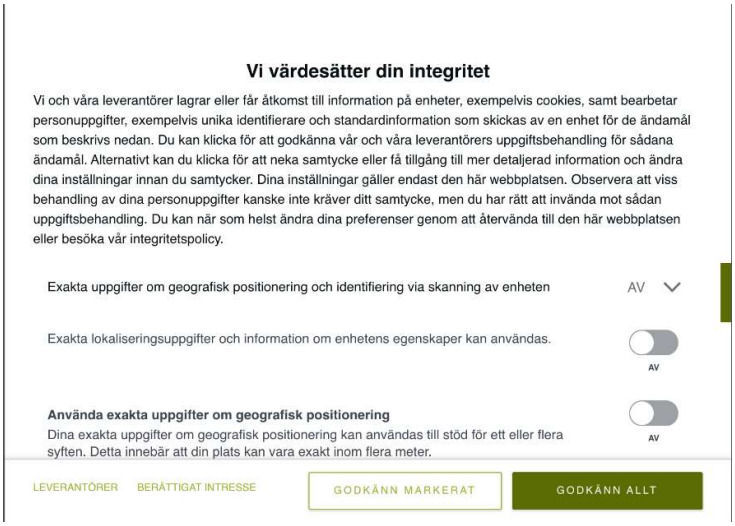

Figure 7. Screenshot of cookie consent example #3 used during the interviews. Source: https://www.allabolag.se/

The fourth theme, *Visualizing trackers*, was designed to discuss further the interviewees' understanding of data collection and data processing, which could help get more in-depth answers to the three RSQs. It consisted of a short LightBeam demonstration illustrating how websites are interlinked via third-party trackers. LightBeam (Figure 8) is a browser extension that creates an interactive network analysis map showing the relationships between third party trackers and the sites one visits (Princiya, 2019). Question 16 (*What are your thoughts about what we just showed?*) was asked to facilitate the discussion.

The last theme, *Closing remarks*, was designed to give the interviewees the opportunity to add more information before ending the interview (Question 17 (*Is there something else you want to bring up about cookie consent notices, or related to topics we have discussed, which we have not talked about?*)

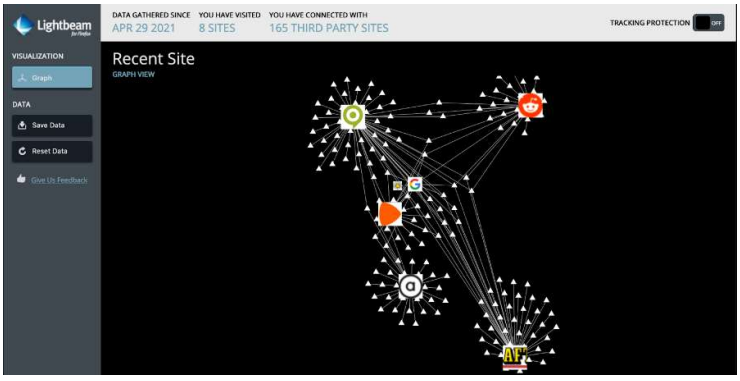

Figure 8. Screenshot of Lightbeam.

3.2 The sample

Sampling in qualitative studies offers different challenges compared to sampling in quantitative studies (Kvale & Brinkmann, 2014). Qualitative studies are not preoccupied with statistical generalizability. A qualitative semi-structured interview study like this one does not need a large sample size to be valid. Instead, other measurements can be applied to determine the validity of qualitative studies. One such measure is data saturation, which can be defined as '*the point in data collection and analysis when new information produces little or no change to the codebook*' (Guest et al., 2006, p. 65).

Naturally, the number of participants needed to achieve data saturation varies from study to study (Fusch & Ness, 2015). As Fusch and Ness point out, study designs are not universal, making a one-size-fits-all method to achieve data saturation impossible. Additionally, analyzing qualitative data is very time-consuming (Saldaña, 2013). Therefore, we chose to follow Karlstad University's sample size recommendation of eight interviewees (Karlstads universitet, 2019).

The population of interest for answering our research question is internet users in Sweden. Theoretically, we could have recruited eight random Swedes who use the internet daily. This could have resulted in a wide range of views and experiences, which in itself is interesting (Rivas, 2015). On the other hand, this sampling method would have hurt the data saturation since we limited the number of interviewees to eight persons. Therefore, we chose to sample a relatively homogeneous group.

Our sample consisted of eight students studying media and communications at Karlstad University. Four students studied Digital Media and Analysis (DMA), and four studied Visual Communication and Design (VCD). The median age of the sample was 22. The gender ratio was split evenly. Table 1 displays the age of the interviewees, the date of the interviews, how they primarily access the internet, and the length of the interviews. Our goal was to gather approximately 30 minutes of material for each interview, per the guidelines set by Karlstad University for media and communication undergraduates (Karlstads universitet, 2019). We chose not to display the interviewees' gender or program affiliation for confidentiality reasons.

Table 1. Description of interviewees

Interviewee	Age	Primarily access the internet via	Interview duration
Interviewee 1 (I1)	27	apps on the smartphone	30 minutes
Interviewee 2 (I2)	22	apps on the smartphone	30 minutes
Interviewee 3 (I3)	22	apps on the smartphone	27,5 minutes
Interviewee 4 (I4)	21	web-browser on the computer	31 minutes
Interviewee 5 (I5)	21	apps on the smartphone	44 minutes
Interviewee 6 (I6)	25	depends on the context: long sessions via web-browser; short sessions via apps on the smartphone	39,5 minutes
Interviewee 7 (I7)	25	web-browser on the computer	34 minutes
Interviewee 8 (I8)	22	web-browser on the computer	21,5 minutes

Because of the COVID19 pandemic, we could not sample in-vivo due to Folkhälsomyndigheten's recommendations. Therefore, we recruited the interviewees via direct messages on Instagram. This counts as a convenience sample since we recruited people who were the most practical to us in our given situation (Messenger Davies & Mosdell, 2006, p. 65). The sample is not representative of a broader population, which does not hurt the generalizability since most qualitative studies are not preoccupied with statistical generalizability.

Even though the participants in our study were evenly distributed from DMA and VCD, it is not our intention to compare the different orientations. However, we did choose the first four men and females to minimize the risk of gender bias. We sent a direct message to around 30 people and chose the first eight who wanted to participate.

3.3 The data collection and transcription

The COVID19 pandemic affected how we conducted our interviews. Zoom was the preferable option given the circumstances since online classes at Karlstad University are taught via Zoom. We made a reasonable assumption that the interviewees' would have access to Zoom and the skills to use the software. All interviews were recorded with the 'record' feature on Zoom. Also, a

second device was used to record the interviews as a backup. Both authors attended all interviews.

The audio was transcribed in the web application oTranscribe. Compared with Nvivo, the advantage of using oTranscribe is the fast and user-friendly interface. It allowed us to transcribe all interviews relatively quickly. We have considered the risks of using the web application, e.g., whether it stores and shares information with third parties. Even though oTranscribe is a web browser application, none of the files leave the computer's hard drive. Everything processed in oTranscribe takes place in the computer's local storage and is never uploaded to the internet (oTranscribe, 2019).

3.4 Thematic coding

We chose thematic coding for analyzing the collected data. Thematic coding, also known as thematic content analysis (Rivas, 2015), is a way of organizing the qualitative data into themes, categories, or patterns (Rivas, 2015, p. 430; Saldaña, 2013). The themes, categories, or patterns are built on codes from the analyzed data material. A code in qualitative research is '*most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data.*' (Saldaña, 2013, p. 3). Coding is a time-consuming endeavor, and one must at some point decide what data to code and what data to set aside (Saldaña, 2013). We chose to code data that could potentially answer the research question and the three research support questions.

The data was coded in Google Sheets because we could not meet up at Karlstad University due to COVID19 restrictions. Initially, we considered coding the data in Nvivo 12. Unfortunately, the program does not work with Nvivo's subscription based Collaboration Cloud (Nvivo, n.d.). Hence, we imported the transcribed interviews into Google Sheets as plain text files.

Saldaña (2013) mentions quite a few personal attributes that are needed for coding. Firstly, one needs to deal with uncertainty, which means that there is no straightforward guide that one can follow. Secondly, one needs to be persistent and be prepared that it takes a lot of time. For example, one will need to be adaptable, given that it might take a few tries and some cycles of coding before one gets it right. Part of the process is that the coding is ever-changing and thus evolving during the procedure. Thirdly, one needs to think in several different ways and be creative, not only during the coding but also during the data collection, analysis, and even in the final written report. One of the most critical skills, according to Saldaña, is to have an extensive

vocabulary. The words we chose to use in the coding are vitally important. For example, there are a lot of different interpretations of different words.

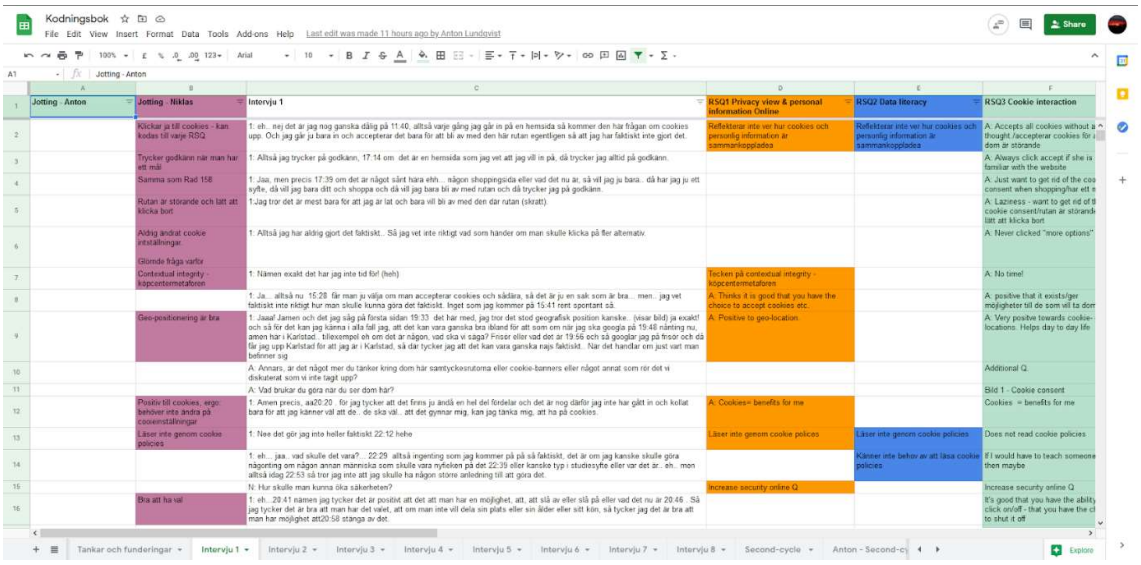

Figure 9. Screenshot of the codebook.

The analytical process consisted of four major steps: first-cycle coding; second-cycle coding; sorting the second cycle codes into categories; and organizing the categories into themes.

3.4.1 First cycle coding

The first cycle coding process involves assigning codes to the collected material. A qualitative code is according to Saldaña '*most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data.*' (Saldaña, 2013, p. 3). Codes help researchers find and categorize similar data units (Miles et al., 2020). Since qualitative data materials usually are information-rich, it is crucial not to forget the study's purpose and research question when coding.

In our coding book (Figure 8), each interview was coded on its own page in Google Sheets. Every page had the same four columns with the RSQs on the right-hand side. The idea behind this was to systematically guide our coding by evaluating if a potential code could answer one of the initial four RSQs. The left-hand side was used for jotting down thoughts and proto-codes before coding the interviews. The first cycle codes were regularly revised and trimmed before moving on to the second cycle coding.

3.4.2 Second cycle coding

For the second cycle coding, the first-cycle codes were placed on a separate Google Sheet page (Figure 9). The main purpose of second-cycle coding in our case was to condense several hundred codes into a smaller number of categories (Miles et al., 2020). We placed the first-cycle codes related to RSQ1 in one column, the codes relating RSQ2 in another, and etcetera.

The second cycle coding stage underwent several revisions. In the first stage, we organized related codes into distinct categories. The second stage involved a more refined organization of the codes. We filtered the codes after their names and performed a second revision of the codes. Certain codes were deleted, some changed categories, and a number of codes were removed.

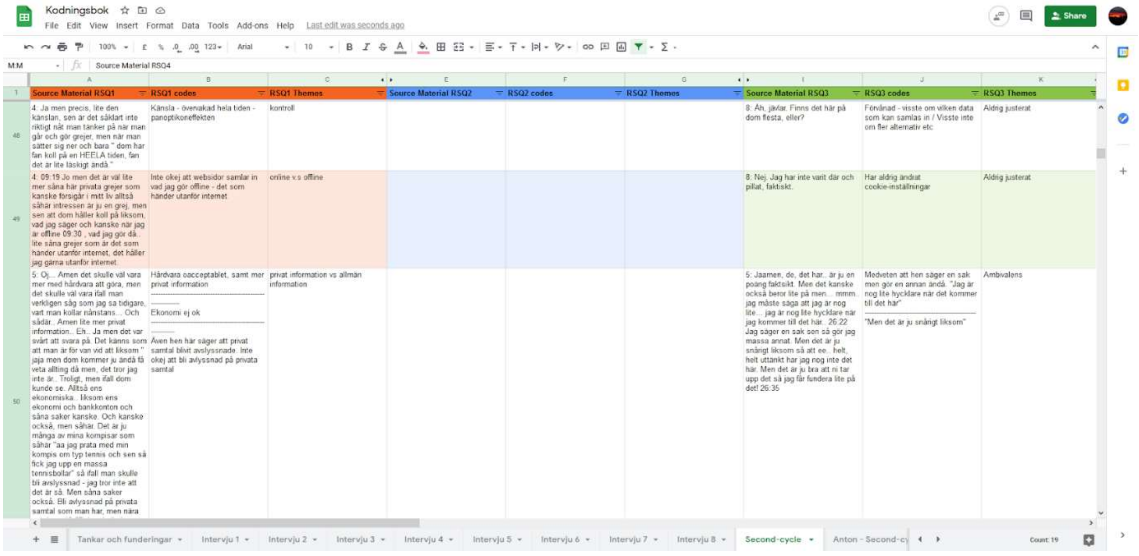

Figure 10. Screenshot of second cycle coding.

3.4.3 Turning second cycle codes into themes

The last step in our analysis was turning the second cycle codes into themes. We used Google Jamboard to sort the categories into themes visually. Like Google Sheets, Google Jamboard has a collaboration function, allowing us to discuss and sort the categories together in real-time.

We utilized axial coding to turn second cycle codes into themes. Axial coding is a method where previously coded data is strategically reassembled (Strauss & Corbin, 1998, p. 124, referenced in Saldaña, 2013). Axial codes look similar to mind maps. The hub, i.e., the axis, is the main category or theme, and the attached "bubbles" are sub-categories or sub-themes. In our case (Figure 10), we used colored-coded virtual post-it notes as codes. The pink note signifies the proto-theme, the green note signifies a sub-theme, and the blue note signifies relevant quotes in our coding book. The circles (themes) and the square (miscellaneous) are just borders keeping the codes

more tidy. The axial coding process underwent several revisions before deciding which themes to keep, combine, and discard.

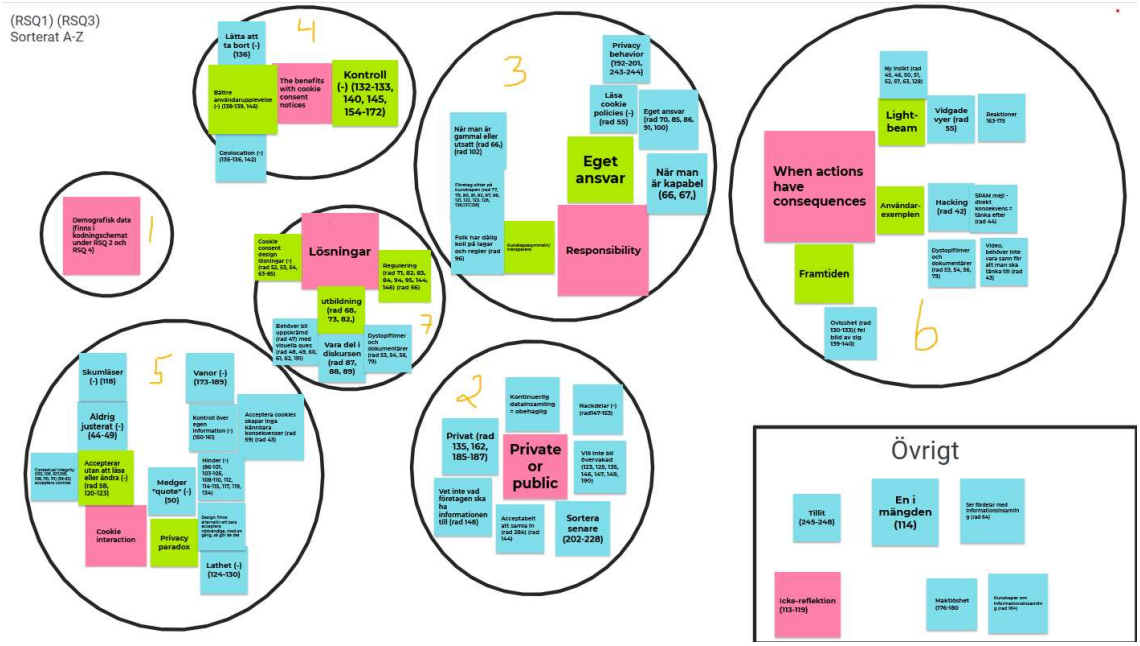

Figure 11. Screenshot of the axial coding in progress.

3.5 Reliability, validity, and Generalizability

The discourse about reliability, validity, and generalizability in qualitative research is polarized (Carminati, 2018). The mentioned terms connote the positivistic tradition of precisely examining and measuring a phenomenon. A faction of qualitative researchers disagrees with using the terms to assess the quality of qualitative research since they are rooted in positivist ontology and epistemology. They argue that qualitative research becomes oppressed when subjected to positivistic terminology (Kvale & Brinkmann, 2014). Additionally, there are few standardized rules for qualitative studies since qualitative studies usually deal with the human experience from an interpretivist perspective (Brink, 1993; Carminati, 2018; Kvale & Brinkmann, 2014; Morse et al., 2002)(Carminati, 2018; Fusch & Ness, 2015)

The other faction of qualitative researchers argues that reliability, validity, and generalizability are vital concepts for assessing the quality of qualitative research (Brink, 1993; Carminati, 2018; Kvale & Brinkmann, 2014; Morse et al., 2002). As Morse et al. (2002) state, all forms of research should aim for rigor if they want to remain useful in a scientific context. We strongly agree with this sentiment, considering that qualitative studies have a particular reputation of being opaque about their methodology (O'Reilly & Parker, 2012). Semi-structured interview studies are subjected to a myriad of factors that can affect the results, such as the interviewer's interviewing

or coding skills (Kvale & Brinkmann, 2014). Being transparent about every step in a study permits other researchers to assess the study and provide valuable feedback.

3.5.1 Reliability

Reliability in the context of semi-structured interviews refers to the consistency and trustworthiness of the results (Kvale & Brinkmann, 2014). Like the quantitative operationalization of the term, a notable aspect of reliability is the reproduction of results: how does the interviewer ask the questions and interpret the results? Are the interviewees' responses consistent, or do they change their answers throughout the interviews?

Good interview studies need attentive interviewers. Body language, tone, word choices, and follow-up questions can shape the interviewees' answers (Kvale & Brinkmann, 2014). Being mindful of these variables is therefore important if one wants to achieve reliable results. In our interview guide, we added examples of follow-up questions to remind ourselves of what topics we wanted to explore. This gave our interviews more consistency by reducing the degree of improvisation when asking follow-up questions. On the other hand, the more rigid interview guide had a dampening effect on the creativity of our follow-up questions, at least to a certain degree.

Since cookie consent notices often differ in design depending on which websites one visits, we chose to show an example of a cookie consent notice to the interviewees as a visual aid. The name *'cookie consent notices*' is also problematic since it is not a standardized term. Showing a picture of a cookie consent makes it easier for the interviewees to recognize what we referred to. The same image of a cookie consent notice was shown and it possessed a number of features that we thought could result in interesting discussions about the designs and purposes of cookie consent notices.

The intercoder agreement, i.e., the consistency between codes made by two or more researchers (Saldaña, 2013) is a good measure of internal reliability. This process highlights what the researchers agree and disagree on, which improves the analysis and the study. Unfortunately, such rigidity takes quite a bit of time. We, therefore, opted for a similar approach for internal consistency, namely dialogical intersubjectivity (Kvale & Brinkmann, 2014, p. 293). The process of dialogical intersubjectivity consists of rational dialogue and mutual feedback, in our case, between the authors. Qualitative coding is a challenge, especially for beginners like ourselves (Saldaña, 2013). Giving each other feedback on our codes was a strategic choice to strengthen parts of the study's internal reliability.

3.5.2 Validity

Validity in the context of semi-structured interviews refers to various forms of quality control throughout the whole study (Kvale & Brinkmann, 2014). According to Kvale and Brinkmann, one approach is to be critical and thorough when designing the study. They bring up seven steps (Kvale & Brinkmann, 2014, pp. 210–213) which we have followed: (1) Our study is built on relevant theories by established scholars and peer-reviewed research. (2) We planned and prepared for the interviews, with emphasis on producing knowledge that will be used for societal good with minimal harm to the interviewees. (3) We have discussed the truthfulness of the collected material (see section 5.4). (4) The translation of the material from spoken to written language is suitable for this study. The same consideration was taken when translating the quotes from Swedish to English. (5 & 6) The analysis and validation of the analysis are grounded in previous research. (7) We are transparent about the study's methodology and results.

3.5.3 Generalizability

Generalizability in qualitative studies is not so much a question of the possibility to generalize the results to a broad population, but if the given results could be applied to similar situations. This study's results achieve *naturalistic generalizability* (Kvale & Brinkmann, 2014, p. 311) as it relies on personal experiences. Our interviewees were allowed to express their answers with their own words and reflect on their own implicit knowledge by the interviews' open questions design. According to Kvale and Brinkmann (2014), naturalistic generalization is based on personal experience. In the process of personal experience and implicit knowledge being verbalized, it transforms into an explicit form of generalizable remarks and statements.

3.6 Ethics

When conducting and writing interviews, there are some ethical situations to consider, according to Kvale and Brinkmann (2014) and the Association of Internet Researchers (AoIR) guidelines (franzke et al., 2020). First and foremost, all interviewees were informed about the purpose of this study. They were then given the option to consent to their participation in the study or to withdraw. Regardless of the relatively uncontroversial phenomena we explored, there were some ethical aspects we had to be aware of when conducting the interviews.

One ethical aspect to consider was the possible power asymmetry between the interviewer and the interviewee (Kvale & Brinkmann, 2014). With this in mind, we aimed to conduct each interview in an engaging and non-invasive way. To battle this eventual power asymmetry, we were meticulous in telling our participants that the study focuses on their view on cookie consent notices and privacy and not their existing (or non-existing) knowledge about the subject. They

were also given the information that answering a question was optional and that the interviews were done in confidentiality, meaning that their names or initials would not be disclosed in the study.

We followed the AoIR's (franzke et al., 2020) recommendations regarding the management of personal information and the study's material. The copies of the recorded interviews were stored locally on our computers. The data analysis and coding sheet were stored on Google Drive, without the possibility to identify any of the participants. We chose Google's platform because of the ability to collaborate remotely.

4. Findings and analysis

In this chapter, we present the analysis of the eight interviews. We have used previous research and theories discussed in Chapter 2 to support our analysis. By conducting a thematic analysis, the results are presented in five main themes in which we further explain our results. The following themes are explained in this chapter: Surfing patterns, Private or Public, Responsibility for one's privacy, perceived usefulness, and Cookie interaction.

4.1 Surfing patterns

When we asked the participants which websites they visit except for social media sites, we got similar results. Everyone mentioned that they visited KAU and Canvas for studies, followed by various online shopping sites and streaming sites. Five of the interviewees primarily use their smartphones as their primary devices to access the internet, and three interviewees primarily used their computers to surf online. While browsing the internet on the smartphone, only one of the participants does it mainly through the web browser, and the rest only access the internet through various apps:

> It is mainly through apps. It is very rare that I actively use the browser. That is just the case if I go through a link that opens, which asks for permission to open the browser, then I use the browser. However, I usually do not actively go on safari and search there. I use existing apps and search through them instead. I do not know why it is like that, but it has just been that way. (I6)

I7's habits were similar:

> Hmm. Sometimes I use the browser. Not very often, in any case. If you look at the screen time and so on, it is clearly apps that are the most. Sometimes I check things on my cell phone if there is anything I need to know. But I have the email and all that stuff through apps as well. (I7)

One could argue that this pattern is related to nudging. It is far less friction to go through apps and consume content almost instantaneously. The other option consists of several steps: first, accessing the web browser, searching for the site, and finally consuming content. (Acquisti et al., 2017; Utz et al., 2019). In terms of nudging, social media apps nudge users to use their apps instead of accessing the services via web browsers.

4.2 Private or public

An aspect of understanding to what extent the interviewees adjust the flow of their personal data on the internet is to explore what information they consider to be private, respectively, public

information. The interviewees' responses resulted in relatively heterogeneous results, meaning that the same type of personal data can be private and public. The answers suggested that the line between personal and public is blurred depending on the context where personal data is collected, which relates to the theory of contextual integrity (Nissenbaum, 2010; Nissenbaum, 2011).

Two frequently mentioned types of personal data were personal email addresses and phone numbers. I1 viewed emails and phone numbers as private because they are used for private activities, meaning emailing and phone calls are private contexts (according to I1's line of reasoning). Processing email addresses and phone numbers go against I1's expectations and are thus viewed as privacy violations:

> Emails in particular, I've noted that I sometimes get, which I assume everyone gets, these spam emails. And I think that happens because some company gets hold of one's email and passes it on to others. Or, if it is phone numbers, I have also got a lot of mail about, or text-messages, about express loans and stuff. So, I guess someone got hold of my phone number and then sent everybody mass-texts. (I1)

I2 expressed a similar argument as to why phone numbers are private: making phone calls is a form of private activity among close family members. However, sharing personal email addresses with websites was acceptable because '*it is something one is used to, like when you register an account … it is just something that has to be shared* (I2). I7 echoed I2's argument with an added emphasis on trust: '*You share it* [your email address] *everywhere, with different webpages. After all, I believe the webpages who are fairly legit do not do anything with it.*' (I7). The standard practice of sharing one's email to register accounts was thus reason enough to consider emails as public information.

The interviewees were polarized on whether personal information is available on websites like Eniro[4]. On the one hand, the information on Eniro was seen as public information: '*I think one's age, gender, hometown, the city you live in, occupation, the kind of more official stuff are ok.*' (I5). Likewise, I4 thought of sharing information displayed in public as non-problematic: '*I'm not particularly worried about names, I still write my name on Facebook, Google, and everything.*' (I4), but was at the same time reluctant to share the home address with websites '*I hope they don't save things like where I live and such. I know that they do so since I've seen it in my downloaded information*' (I4).

[4] Eniro is a Nordic technology company engaged in, among other things, digital marketing, maps, and telephone directories for businesses and private persons. https://www.eniro.se/

Being monitored in the physical world made most of the interviewees feel uneasy:

> it isn't very comfortable … that it [trackers] can view all where I've been with my phone … it feels like they keep track of you … it doesn't feel like you're really alone. It feels like someone always knows where you are, and you feel like 'just let me live my life in peace (I4)

This case was especially important when tracking takes place outside of their control, such as offline tracking or unwarranted voice recordings: '*I don't remember exactly what we talked about, but I got advertisement about the exact thing we had talked about*' (I3). Another reason why personal data was considered to be private relates to uncertainty about websites' use of personal data: '*they frame it like they need this* [data and personal data]*, but why? Yet, they cannot give an answer to "why"*' (I6). I8 echoed a similar argument 'I *don't really know why they want to have this information*' (I8).

These thoughts could be related to Westin's (1967) arguments about control over personal information. When users feel that companies collect personal data without being transparent, they subsequently feel a loss of control over their personal data and become hesitant to share it with companies.

4.3 Responsibility for one's privacy

The theme responsibility comprises different attitudes about the interviewees' reasoning about who has the greatest responsibility for protecting internet users' integrity. The GDPR puts most responsibility on website owners to be transparent about their data processing, but the internet users also have a responsibility to give *informed* consent ((EU) 2016/679, s. 6). The interviewees were divided on the issue. On the one hand, the individual bears the uttermost responsibility for protecting their personal integrity, which Westin (1967) would argue. On the other hand, the interviewees also expressed that there are asymmetries between regular internet users and website owners, which aligns with arguments made by proponents of political economy(Andrejevic, 2014; Jin, 2021)

4.3.1. Sub-theme: personal responsibility

The interviewees who argued for personal responsibility did so in two distinct ways. Two interviewees argued that one must be careful about what one uploads on social media because these actions can have consequences. I7 said '*I don't know. I'm a bit unsure. Because I think a hell of a lot of people post so much shit without thinking about it, so I think "you can only blame yourself. You're just stupid"*' (I7). I6 shared similar sentiments: '*I think that one should want to learn* [about privacy on the internet], *one should want to educate oneself*' (I6), but added that posting personal musings online is acceptable if one is as open offline. These arguments are similar to Westin's (1967) approach to

privacy. Both emphasize the importance of personal responsibility for protecting one's privacy, i.e., being mindful about what information one shares with other parties.

The second way personal responsibility was expressed differed considerably from I6's and I7's. Instead of focusing on the individual's responsibility to protect one's privacy, I8 addressed the need for collective efforts from internet users to help each other protect everybody's privacy. I8 mentioned writing reviews as a method to inform others about '*sketchy sites*', although '*something I'm bad at is, like, if I discover something that is actually sketchy, writing a review about it, or something.*' (I8). The collective aspect of personal responsibility differs from Westin's (1967) theories, which emphasizes the importance of individuals taking control over their own information.

4.3.2 Sub-theme: the disadvantaged

Every interviewee expressed in some form that there is a knowledge asymmetry between internet users and website owners, an argument highlighted by, e.g., Andrejevic (2014) and Kennedy (2016). The elderly or children were frequently used as examples of people at a disadvantage because they cannot comprehend how the internet works:

> I think it is every person's responsibility [to protect one's privacy], but I also think certain people have a hard time [protecting their privacy]. Personally, I'm at least a bit knowledgeable about this, I'm still a bit up to date on what is going on. But then I think about an elderly person who doesn't know what is going on, who has gotten a laptop or a tablet and who does not know what is going on … There should be more assurance for these kinds of people, I would say. (I1).

The interviewees pointed out that they felt like they knew enough basic information to be able to surf the web. A few of the interviewees pointed out that it was one's own responsibility regarding what and how one surfs online, akin to Westin's (1967) notions of privacy. However, when they were given a follow-up question if the elderly should also be responsible for each and every action while also being well-informed - most of the interviewees said that there should be some kind of regulation/assistance online. These arguments came across as a mix of notice and choice (education) and political economy (regulation). Additionally, I3 explained that children should get some kind of education regarding privacy:

> Yeah, and then it is not as clear then... I guess the current system is okay. But I think that some kind of introduction should be introduced at an earlier age. I can imagine that children today access the internet way easier than we all did. So I think it's more about an earlier form of education. (I3)

Promoting education in order to improve individuals' digital literacy has been suggested by, e.g., Park (2013). In contrast, I6 thought the root of the problem instead lay in how complex the current system is, referring to the knowledge asymmetry between ordinary internet users and big tech companies and websites (Andrejevic, 2014; van Hoboken, 2019):

> Yes, but do it more [understandable ToS/GDPR] for everyone, because now it feels significantly advanced and challenging and only a particular dignitary person understands it. It feels like someone on, well I do not want to mention companies, but someone on a big-tech internet company has decided that this is supposed to be "very difficult. And that only we should understand. We should benefit from this." It feels that way anyway. And it makes us, I was about to say, peasants. But I mean, we, as in the civilization, do not understand because we are not up there. But that it just feels like someone has made it complicated. And someone needs to questions why and get it to be more normal because there will be even more of GDPR ten years from now. And by then, everything will also need to be approved, and yeah, that's a whole discussion, but I believe that we have to get it more simplified. (I6)

4.4 Perceived usefulness

Although not a form of interaction, the theme is still important. All interviewees said that cookie consent notices give internet users the option to control websites' processing of personal data, which coincides with the ambitions of the GDPR. For example, I1 said '*I think it is good that you have the option to not share one's geolocation, or one's age, or one's gender, so I think it is good that you have the option to turn it off.*' (I1). The interviewees felt cookie consent notices could empower internet users by letting them be in charge of their own decisions:

> They have the opportunity to take a stance to it [accepting cookies or not] and ask: 'okay, what am I ok with? And not, as you said before about feeling powerless, instead feel that you have some, some agency in this as well. And I think this is important, both for the individual, but also for us as a species, to feel that we have agency over ourselves, and feel that we can make our own decisions. (I6)

One of the interviewees clearly said they felt like cookies probably benefit them to a high degree. Accepting all cookies adds more convenience to daily life:

> I think there are a bunch of benefits, which is why I have not even bothered to check the settings. Because I think well, I imagine that it benefits me to have cookies… I think that [accepting] geographical position can be pretty good sometimes because when I'm about to google something now here in Karlstad for instance, for example, "hairdresser" when I google that I get the results in Karlstad because I'm in Karlstad so I think it can be pretty nice actually when it comes to exactly where you are.(I1)

This was followed by a rather frequent saying we heard from all of the interviewees. They pointed out that having the choice and reading what you accept is preferred compared to several years ago when cookie consent notices did not exist:

> It is positive that you in some way approve of it yourself. Even though you do not really read it, I mean, if you would just have been thrown directly into the website and they take your data – that would not have been very convenient. Now it is still like, "Okay, I have accepted, and I'm fully aware that I give them my data." So it becomes more positive and nicer. You cannot really complain about anyone other than yourself when you approve of that kind of stuff. (I4)

An observation we made during the editing and coding process was that the interviewees were optimistic that reading more about different policies exists. Despite this, practically everyone said that they do not read privacy policies. The interviewees in our study appreciated that the option exists since it could increase the overall awareness. Nonetheless, (basically) none of the interviewees adjusted their cookie settings regularly when interacting with cookies.

4.5 Cookie interaction

We noticed several different sub-themes during the coding process regarding how the interviewees interact with the cookie consent notices. There were some mixed results in regards to the interaction. Most of them accept cookies without reading the cookie consent notice for various reasons, such as habits, the cookie design, and previous experiences.

4.5.1 Sub-theme: habituation

Interestingly, despite the interviewees' praise for the cookie consent notice as a helpful privacy tool, none of the interviewees regularly adjusted the cookie settings, and few had read cookie policies outside a classroom setting. When we showed the interviewees the first cookie consent image (Figure 5) the majority said they would click accept without batting an eye: '*Oh, oh, I* [click] *accept right away*' (I7).

The phrase '*I'm a bit lazy*' and similar sentiments were expressed noticeably often. It seems like the interviewees did not reflect too often on the consequences of accepting cookie consent notices. The following quote was the response to our question of why I2 accepts cookies without adjusting the cookie settings: '*It happens automatically, you are so goddamn used to it. So, you don't think about it*' (I2). I3 stated similarly:

It is a bit of a habit [accepting cookies]. I think they have been around for a couple of years, I am also thinking about those younger than me. When you notice that you can continue [to the

website], it will probably become a habit that you just accept without thinking about the consequences. (I3)

A common response was that accepting cookies had become a habitual response. Whenever most of the respondents go to a website, they quickly accept without really thinking about it. One reason could be rooted in trust: *'Quickly press approve, yeah – without actually reading through the whole thing. You think it should be right and work in the right way, so then you are not so worried about it as well.*' (I3)

Another respondent mentioned that they have not really cared about their privacy at all and have never had any negative consequences while using the internet:

> I have been accepting all of this stuff and have not cared about integrity at all since I started using the internet. And I mean, I'm still sitting here today. I have not ended up in any prison, well, you know what I mean, there haven't been any consequences before, I have never been hacked before. (I7)

Regarding what would be needed for the interviewees to some extent read the cookie policies. A shared saying amongst some of the participants was that if they knew it would affect their life in some negative aspect, then they might consider reading it:

> If I would have known that the decisions I make now, if they have any impact on my life in a negative way, then I might have considered reading through it first. If I had known all of the consequences beforehand, then I would have known whether I made the right or wrong decision. (I4)

After some of the interviewees were asked a follow-up question, what could be improved upon the knowledge gap on privacy, two interviewees suggested that more documentaries or movies should be aired on the subject of teaching privacy. Documentaries similar to the Social Dilemma were mentioned both times. *'We watched the Social Dilemma this fall, then everyone was very paranoid for like a week, but nothing has changed since.'* (I5). Commonly mentioned was that watching or learning something about their privacy gives them the urge to change their habits and, in some way, become more aware of their integrity.

However, it seemed that after a few days to some weeks, that worry disappeared completely, and the interviewees were back into old habits. This also seemed to be the case for those few interviewees who had seen LightBeam before. Even though they had seen it before, they said that it did not change their surfing behavior in the long term. This was also supported by a finding

from Obar and Oeldorf-Hirsh (2020), which suggested that users easily develop habits and quickly go back to old patterns, even if shortly interrupted.

4.5.2 Accepting only essential cookies when given a choice

Apart from only accepting cookies blindly, we found out that several of the interviewees made a conscious decision not to blindly accept them when there was another option immediately shown when the cookie consent notices appeared.

The question regarding what the interviewees do when they encounter a cookie consent notice (similar to Figure 1) gave mixed results. Although most interviewees said that they click accept immediately, some of them were aware that certain cookie consent notices offered the choice of only accepting essential cookies: '*The fact is that it usually happens if there is only accept* [always accept if that is the only choice]. *However, if there exists an option not to approve, then I click on that option*.'(I7) Another interviewee answered: '*Yes, I have done it a few times, or well, I click on the "accept only necessary cookies" when I'm given the choice.'*(I2)

A typical pattern with half of the interviewees was that if they were immediately given a choice to accept only necessary cookies, they occasionally did that most of the time. What also emerged was that the interviewees who accepted only necessary cookies when the option was given felt like the websites have made it impractical to customize cookies:

> Some have the option to approve only necessary cookies, then I usually go for that. So I always try to think about what I do or how much of my data I accept that they take and if it is necessary that they actually have so much of my data when I only am visiting a website once.(I4)

Finally, in one of the interviews, a seemingly uncommon design was mentioned, '*I think Eniro has one button where it says, 'decline all cookies,' which is quite rare, but nice!'* (I5) which is the option to *accept* or decline by a '*decline all cookies'* choice.

To our knowledge, most websites do not have the "Accept only necessary" cookies option available. The absence of "Accept only necessary" means the users are nudged into clicking "Accept all" cookies (Acquisti et al., 2017; Utz et al., 2019). As previously stated, most of the interviewees want to get rid of cookie consent notices quickly, and adjusting cookie settings takes a bit of time. Arguably, websites without "Accept only necessary" limit (intentionally or unintentionally) the users' agency over the flow of their personal information. This is a problem related to political economy (Jin, 2021) and contextual integrity (Nissenbaum, 2010; Nissenbaum, 2011).

4.5.3 Contextual acceptance of cookies

Accepting cookies was not solely an automatic habit or a result of binary choices. I5 recognized that certain occupations rely more on advertising revenue than others, like journalists and bloggers:

> And it is like this [data collection] in certain occupations, it's how they finance everything… newspapers have gone online, but I don't want to pay for this. But, people have this as an occupation too … but you can pay with your personal information instead of your paycheck. (I5)

I5 states that data collection is acceptable if the websites serve societal functions. Websites like SVT (Sveriges Television Aktiebolag, part of Sweden's public service), Yr.no (Norwegian weather forecasting website), and 1177 Vårguiden (Swedish healthcare service via telephone and the web) provide services which benefit society on large: '*SVT, Yr.no, 1177… they are kind of the good guys.*' (I5). In contrast, web forums like Flashback (Swedish internet forum) and questionable (from I5's perspective) online newspapers like Nyheter 24 should not have access to I5's personal data.

I5's reasoning resonates with Nissenbaum's (2010; 2011) construct *context-relative informational norms* of contextual integrity. The construct states '*key parameters of informational norms are the actors (subject, sender, recipient), attributes (types of information) and transmission principles (constraints under which information flows).*' (Nissenbaum, 2011, p. 33). I5 has different expectations of how personal data is processed depending on I5's perception of social good. For example, SVT or 1177 are allowed to collect personal data since their services contribute to the improvement of Swedish society, while Flashback or Nyheter24 do not. So, the fact that these aforementioned sites collect personal data goes against I5's expectations and is thus viewed as privacy violations.

4.5.4 Coercion

Furthermore, some interviewees accused website owners of purposefully creating an environment where the internet users are at a disadvantage by convoluted design choices: '*they are so complex* [cookie consent notices]*, it should not take five steps for me to, and take five minutes to read what they* [the websites] *what they use… and they know this.*' (I7). The length of the text on cookie consent notices were also criticized for being too long '*The negative aspect of the cookie boxes is that there is far too much text, and no one has the energy to read it.*'(I4) , and too complex: *'They want you to accept… If they write it in a more advanced way, then everyone will not understand it. I think it is negative that they adjust it to suit them.*

Convoluted cookie consent notice designs and interruptive properties associated with cookie consent notices cause frustration, which in a way forces the interviewees to accept cookies even though they not necessarily want to:

> You often go to a webpage because you want to get hold of something, and this [sic] cookies, it becomes an obstacle, and you, of course, feel a bit of frustration, and then you just want to move forward. (I5)

Two interviewees argued that cookie policies should instead be similar to children's books, suggesting improvements in line with ideas from Privacy by design (Cavoukian, 2009, 2011):

> Just simplify it to make it easier to understand to the average internet user ... If it were designed like a damn children's book, with easy-to-read colors and so you could read it in ten seconds, then I would read the policies. (I7)

I5 used the same argument: *'The visual aspects are important if it was more like a children's book instead of a novel, that would make it easier for me to read.'* (I5)

Another aspect of coercion is the fact that (anecdotally) certain websites can block users from accessing their content if they do not accept cookies. I8 experienced this a few times before, and thus chose to continue accepting cookies:

> In my case, I accept things that I don't know about. Like position and all of that. And, as we talked about, that certain website requires you to accept cookies to access their sites. And then, even though it can be viewed as a choice, it isn't really a choice, in my opinion. Because you still have to click 'Accept' if you want to access it [the website]. (I8)

I8's experience with websites that "forces" you to accept all cookies in order to be able to access the website in its full functionality refers to political economy. The two choices are either accepting all cookies to gain access to the website or declining cookies and being unable to either use the website or use it with very limiting functions. For example, they will not be able to play videos or read specific content. From a political economy perspective, these options are unreasonable and only strengthen the power asymmetry between website owners and internet users (Andrejevic, 2014; Jin, 2021).

In most cases, the interviewees experience the design and functionality of cookie consent notices as coercive. However, one interviewee noted that cookie consent notices themselves are not the real issue: *'So I do not really think the issues about the windows [cookie consent notices], I think it's more about how they [website owners] use the data*'(I4). I4 would instead see more regulation regarding personal data collection and processing, similar to, e.g., Andrejevic (2014) and van Hoboken (2019).

4.5.5 Adjusting cookie settings

One of the unique insights into how the interviewees interact with cookie consent notices was that only one interviewee reported adjusting the cookie consent notices. The action was performed as a privacy measure to get more insights into unfamiliar websites' data collecting and processing. I6 acknowledges that reading through the cookie settings takes time, and it is worth the effort in given situations:

> It depends on the website. If it is a page that I am on often, then I just approve it. However, if it is a webpage that I am a little more unsure of and a page I usually don't visit, then I click on more options to see it more clearly. I also need to have the time… If I just want to check something quickly then I might not put in the effort. However, if I am unsure, I usually click on more options because I do not want a page I rarely use to see what I am doing. (I6)

I6 was the only participant from our interview that adjusted the cookie settings with the purpose of controlling the flow of personal data. I6 makes in certain situations conscious decisions to limit third-party access to I6's personal data, which relates to Westin's (1967) theory about notice and choice.

5. Discussion and conclusion

This chapter will discuss the findings and analysis in relation to the literature and theoretical framework presented in Chapter 2. The discussion is centered around the study's purpose, research question, and research support questions. The chapter also consists of the validity and limitations of the study, as well as our conclusion.

5.1 How do internet users access the internet?

The majority of the interviewees accessed the internet via their smartphones, and social media was one of the web services the interviewees used most frequently. These findings reflect the general trend in Sweden (Andersson et al., 2020; Internetstiftelsen, 2019). Social media was used predominantly via smartphone applications. We argue that the trend of accessing the internet via smartphones and smartphone applications is troublesome when viewed from the lens of political economy.

Firstly, smartphones and smartphone applications collect a substantial amount of personal data. A study by Papadopoulos et al. (Papadopoulos et al., 2017) showed that both web browsers on (Android) smartphones and smartphone applications leak identifiers (data) to third parties. The identifiers examined in this study include GPS coordinates, Advertising ID, operating system (OS), smartphone manufacturer, smartphone model, and screen resolution. The Ad-block browser, which is promoted as an option for the privacy-minded, also leaks data (advertising ID, OS, smartphone manufacturer, and screen resolution). Google's trackers google-analytics (used for web analytics) and doubleclick (used for advertising) tracked 56 percent and 53.6 percent, respectively, of the 116 sampled applications. Facebook tracked 50.4 percent of the sample.

Secondly, users have few options but to comply with the tracking taking place on their smartphones. In contrast to services accessed on web browsers (to our knowledge), (Android) smartphone applications seldomly display cookie consent notices (Mehrnezhad, 2020). The absence of cookie consent notices, or other tools that allow adjusting the flow of personal information, perpetuates the power asymmetry between service providers and users (Andrejevic, 2014; Nissenbaum, 2010). Arguably, the usefulness of cookie consent notices relies in large on how users access the internet. If the majority accesses the internet through apps, cookie consent notices fall flat since users would be less exposed to access them (Mehrnezhad, 2020).

The haphazard use of cookie consent notices in smartphones leaves the users with two realistic options: agree to our terms of condition or stop using our services. The intertwining of smartphone applications and daily life in Sweden (Andersson et al., 2020) boils down the options

even further: accept the terms of services and take part in society, decline and struggle. However, our results suggest that more cookie consent notices on smartphone applications would not improve the situation: users would still click "accept all cookies" to get rid of the messages. Arguably, more cookie consent messages would instead legitimize the already unsustainable collection and processing of personal data.

5.2 What are internet users' perspectives on privacy on the internet?

During the interviews, we noticed that the interviewees had mixed judgment regarding their and others' privacy on the internet. While some were quite positive towards the current system, some were more critical towards present privacy policies and regulations.

5.2.1 Few take personal responsibility

We noticed a paradox regarding the interviewees' actions compared to their thoughts and ideas regarding their perspectives online. For example, a few interviewees said that it is one's responsibility to educate oneself regarding one's online privacy, which relates to Westin's (1967) theories. Paradoxically, the same interviewees seemed to agree that there is a lack of transparency regarding the corporation's data collection while stating that they almost never change the cookie settings. This clearly goes against the theory of notice and choice - if anything, the interviewees would have adjusted cookie settings because they are skeptical toward how websites collect and process personal data.

A consistent theme/saying throughout the interviews was that the interviewees felt that the privacy policies were too complex to comprehend quickly. Some even pointed out that the cookie consent notices should be as simple as a children's book. If that were the case, the likelihood for them to read would thus increase. In addition, the attitude towards more regulation regarding privacy policies with the user's privacy in focus was a big topic. For example, the interviewees said that there should be some higher authorities in control of protecting the individuals, which is similar to nudging in the form of Privacy By Design by Ann Cavoukian (2011), which aims to enforce more extensive privacy standards with the individual users in focus.

5.2.2 Feelings of surveillance and uncertainty

The majority of the interviewees pointed out that they felt like big tech companies were monitoring them. At the same time, some of them said that it did not matter at all and that it could have positive aspects of improved usability on different apps. While in some cases, the situation mattered, related to Contextual Integrity (Nissenbaum, 2010; Nissenbaum, 2011). Other

interviewees indicated that they felt uncomfortable with knowing that they were being 'spied on' 24/7. Having that in mind, the interviewees also expressed that they felt uncertainty with the amount of data collected. In addition, they were skeptical of what the use-case of the data has in the future in the long term. Despite their concerns regarding the surveillance aspect, it could be reasonable to assume that the users would adjust the settings as they are aware of it. However, that is not the case, which contradicts Westin's (1967) theory of notice and choice.

5.3 How do internet users interact with cookie consent notices

As previously stated, Westin's (1967) ideas about privacy, notice, and choice do not seem to resonate well with our interviewees in practice. None of them adjusted the cookie setting on a regular basis. All but one were critical toward data collection and processing, and a majority expressed concerns about geo-location tracking. Paradoxically, all praised the cookie consent notices because they allow users to control the flow of their personal data. At first glance, being concerned about one's privacy and accepting cookies without adjusting them seem contradictory. This finding fits the general description of the phenomenon known as the privacy paradox, i.e., being concerned about one's privacy and engaging in behavior that compromises one's privacy (Kokolakis, 2017). However, the analysis suggests that the seemingly paradoxical behavior might be rooted in rational decisions.

5.3.1 Cookie consent notices reward swiftness and punishes diligence

One explanation why the interviewees mostly click "Accept all cookies" is because it is a learned behavior. The findings in the section 'Habituation' align with Obar and Oeldorf-Hirsch's study about privacy policies and clickwrap interaction (Obar & Oeldorf-Hirsch, 2020). In that study, one participant noted how not reading privacy policies felt like a cultural norm. The authors hypothesized that the normalization of accepting privacy policies or cookie consent notices without reading them could result from habituation, based on results from a study by Böhme and Köpsell (2010). The researchers argue that "one click and they disappear" feature of cookie consent notices teaches users to accept cookies automatically. Cookie consent notices ubiquitous presence on the internet can very well "train" internet users to accept cookies automatically. We want to expand Böhme and Köpsell's (2010) hypothesis by proposing that habituation, in the context of cookie consent notices, is a result of rewards and punishments.

The design of cookie consent notices incentivizes, unintentionally or intentionally, users to auto-accepting cookies by rewards and "punishments" in the form of time saved or spent. If a user wants to change the cookie settings, he or she must first spend time reading about the various cookie settings. The average number of third-party cookies present on a website is around 17

(Englehardt & Narayanan, 2016). If the website follows the GDPR's transparency principle, the user should have the option to adjust the settings of all of the third-party cookies. If the user has little to no prior knowledge about the cookies and how they are processed, they must gain that knowledge. Even if the user has prior knowledge about data processing, repeating the steps of reading and adjusting cookie settings still takes time and effort (Choi et al., 2018; Obar & Oeldorf-Hirsch, 2020).

Comparatively, accepting cookies without adjusting them rewards the users by making the dialogue windows cease to exist. The fact that cookie consent notices can act as walls or obstacles hindering the users from accessing content is incentive enough to click accept without reading or adjusting the cookie settings. Another factor why accepting cookies without adjusting the cookie setting "rewards" users is the lack of perceivable consequences of doing so. Besides getting rid of the cookie consent notice, clicking 'Accept' does not visually (or in some other way) indicate how one's personal data is processed. As I7 pointed out, accepting cookies has not radically affected I7's life.

5.3.2 Few to no options

All of the interviewees expressed frustration regarding the general design of cookie consent notices. The interviewees felt that websites purposefully pressured them to accept cookies, echoing arguments used by political economy scholars. (Andrejevic, 2014; van Hoboken, 2019). The almost dichotomous design of either accepting the cookie policies or leaving the service was recognized as unfair. Adjusting cookie settings was not seen as a proper option: reading complicated texts, or spending minutes on cookie adjustments go against their expectations of accessing content or services instantaneously. This aligns well with Nissenbaum's (2010, 2011) perspective on contextual integrity.

Other than political economy, having no options can also be related to nudging, in which a few interviewees explicitly said that they feel forced to accept cookies. In addition, some interviewees said that they feel uncomfortable clicking on more options because it might result in a more complicated text to read.(Acquisti et al., 2017).

5.3.3 Hurdles

Many of the interviewees were annoyed by cookie consent notices because they interfere with their online errand: '*the question about cookies appears every time I visit a website. And I just go in and accept it, just to get rid of this window*' (I1). From the perspective of contextual integrity, online and offline

behaviors are not mutually exclusive (Nissenbaum, 2011). The expectations when shopping for clothes do not change drastically if the activity occurs in a real store or on a computer screen.

Therefore, being greeted with a cookie consent notice goes against one's expectations since this phenomenon is unique to websites: '*the thing is that I don't want to waste five minutes reading a text before I can visit a website*' (I4). Obar & Oeldorf-Hirsch (2020) got a similar sentiment from one of their participants when discussing clickwrap and privacy policies: '*I don't have time to read Terms of Service agreements for every site that I visit*' (Anonymous, Obar & Oeldorf-Hirsch, 2020, p. 142). In other words, cookie consent notices are hurdles that one most easily circumvents by clicking accept.

5.4 Validity and limitations

5.4.1 The interviewees

There is a long tradition of sampling (often under-graduate) university students within the social sciences (Peterson & Merunka, 2014), including communication research (Basil, 1996). The common criticism of sampling students is how it hurts studies' external validity (Peterson & Merunka, 2014). External validity is a whole topic in itself, but the short description of the concept encompasses how findings can be generalized from a smaller population to a larger, or across settings or populations (Lucas, 2003). University students are a part of the adult population, but also differ in terms of factors like cognitive skills (Basil, 1996; Wintre et al., 2001). Basil (1996) and Lucas (2003) do not claim that sampling university students is useless; rather, one should be careful about interpreting and generalizing results from university student samples.

In our study, the sample consisted of media and communications students. It is not unreasonable to assume that the interviewees had more knowledge about the internet compared to the population as a whole, considering the intertwining of media and the internet over the past three decades. Also, the age of the interviewees is, with high certainty, an influencing factor. Older or younger interviewees would have probably given us different answers compared to the answers we got from our sample, because of how they have experienced the technological development differently.

With these factors in mind, the results from our study demonstrate that a sample that is expected to be more knowledgeable "fail" to protect their privacy by adjusting cookie settings. Because of this, the study's findings arguably strengthen the case of increasing data processing regulation over increasing the use of notify and choice to protect internet users' privacy.

It is possible to question the truthfulness of the interviewees' statements (Kvale & Brinkmann, 2014; Rivas, 2015). Like all kinds of research in human sciences, the results can be biased (Rivas, 2015). For example, the interviewees might have given answers they thought we wanted, known as social desirability distortion (Richman et al., 1999). This is an especially important point considering the fact that both the authors and the interviewees belong to the same student organization. Another issue is the difference between actual behavior and self-reported behavior (Jensen et al., 2005). However, we argue that the interviewees' experiences are valid, despite the pitfalls of inquiring knowledge via face-to-face interviews. Their experiences with cookie consent notices corresponded with results from research exploring similar phenomena such as users' interaction with clickwrap (Obar & Oeldorf-Hirsch, 2020), and users' perspectives on data-mining (Hargittai & Marwick, 2016; Hinds et al., 2020; Kennedy et al., 2017).

5.4.2 The interviewing process

An issue during the interview process occurred when we gave some examples about data tracking. Some interviewees got caught in a "loop", where they got stuck on a subject like geo-location and tracking computer-mouse movement, for example, which can affect the study's validity. We could have counteracted this by preparing better examples, more suited for interviewees who are not as familiar with the subject as us. In addition, we noticed during the coding of the data that we could have asked better follow-up questions. We had relied too much on the interview guide for follow-up questions (Kvale & Brinkmann, 2014, p. 180).

5.4.3 The coding process

Our coding process has some strengths and weaknesses. One obvious weakness is that we are beginners. It was our first time interviewing and coding. The codes were constantly changing as a result of becoming better at coding. The thematization changed over time, and new patterns were discovered, and others were discarded. When we reread our codes, we noticed places where we could have improved and made our codes even more focused. Then there is of course the issue of determining what data to code and what data to leave (Saldaña, 2013). Nonetheless, our theoretical framework has guided the design of the interview guide and the coding process, which contributes to the study's validity.

Another issue we encountered, which has more to do about implementing codes into the running text, was the translation of the codes from Swedish to English. The interviewees' use of idioms and informal speech made the texts a bit cumbersome to translate.

A strength regarding our coding is the study's dialogical intersubjectivity (Kvale & Brinkmann, 2014, p. 293) Saldaña (2013) mentions several critiques against coding, for example, there is a risk that one might become distanced from your data. Saldaña backs it up by supporting that coding well requires one to reread and recode the codes several times, making one more knowledgeable about the data.

5.5 Conclusion

The answer to our research question (*What reasons do internet users have for accepting, declining, or adjusting cookie settings?*) is that the interviewees' reasons varied quite a bit. There were a couple of interesting outliers. Firstly, one interviewee did adjust the cookie settings when websites were perceived to be untrustworthy. Similar findings were reported by Kulyk et al. (2018) and Utz et al. (2019). Secondly, one interviewee's argument for supporting websites by sharing personal data has been reported in Kennedy et al.'s (2017) study, which deals with the concept of fairness.

However, the bulk of our findings and analysis suggest that the interviewees seldomly adjust the cookie setting because they viewed them as annoying obstacles, slowing down the consumption of content and use of online services. These results align with studies exploring similar topics (Hargittai & Marwick, 2016; Kulyk et al., 2018; Obar & Oeldorf-Hirsch, 2020), i.e., internet users seldomly read privacy policies or interact with cookie consent notices to adjust the flow of their personal data. Instead, they most often accept terms of services and cookie policies as quickly as possible.

The interviewees could consider reading the cookie consent notices if they changed drastically in design. On the other hand, the requested design overhauls would render the cookie consent notices almost useless. Less text means users will not fully comprehend the complexity of personal data processing (Nissenbaum, 2011), forcing websites to implement more menu diving to comply with the GDPR. Less text or better graphics would not change the fundamental flaws of notice and choice. Moreover, cookie consent notices have arguably minimal impact in today's media landscape. A significant portion of the web activity takes place on smartphones and smartphone applications, where cookie consent notices are mostly absent (Andersson et al., 2020; Internetstiftelsen, 2019; Mehrnezhad, 2020; Papadopoulos et al., 2017)

In conclusion, legislators and policymakers should focus on regulating how personal data is processed, rather than pushing the responsibility of safeguarding personal data onto the users: a notion supported both by users and scholars (Andrejevic, 2014; Kennedy, 2016; Nissenbaum, 2010; van Hoboken, 2019).

6. Future studies

Future studies should explore how much time users spend on smartphones via applications, as well as which applications they most frequently use. There seems to be an issue of illegal (or at least opaque) collection and processing of personal data taking place on mobile platforms (Mehrnezhad, 2020; Papadopoulos et al., 2017). Unfortunately, there is no current statistical data about the number of hours the average Swede spends on the smartphone. This grey area should be investigated further, considering how integrated smartphones are in most Swedes' daily life (Andersson et al., 2020). Future findings will hopefully give valuable insight which can be used to evaluate the effectiveness of cookie consent notices. After all, cookie consent notices' potential becomes lost if users circumvent them by using applications (unless cookie consent notices become the norm in mobile applications).

Future studies should also investigate different populations. The sample in our study was limited to eight media and communication students at Karlstad University, aged between 21 and 27. Quantitative studies could use our findings as constructs and statistically test them against variables such as age, gender, education, and internet experience. Robust, representative studies of how users interact with cookie consent notices are sparse, and more research is needed before we can with certainty evaluate the usability of the latest iteration of notice and choice on the web.

7. Implications for society

The study's findings and analysis show that the majority of interviewees do not adjust cookie settings when interacting with cookie consent notices, despite being reasonably aware of the downsides of personal data processing. Their experiences with cookie consent notices are, for the most part, negative. The dialogue window is a nuisance standing between them and the desired content. Hence, instead of taking control over the flow of their personal data, they often accept websites' cookie policies without hesitation. Cookie consent notices can be altered, new information can be added or retracted. Nevertheless, in the end, internet users want to access services and content without delay. Rebranding or redesigning the dialogue window will not change this behavior.

In addition to the results of other studies, our results should be a wake-up call for legislators and policymakers. The well-meant intentions of notice and choice do not match the reality of how internet users think and behave. It is unreasonable for legislators and policymakers to push the burden of responsibility for one's privacy almost exclusively onto the internet users. Notice and choice on the internet are only useful if users comprehend how the internet works and the various laws governing the internet. Simply put, the internet is too convoluted to break down for the average internet user.

The study's findings support the notion of increased regulation regarding how and what personal information second and third parties can collect and process. The "everything goes" attitudes expressed by the major technology companies about personal data are not sustainable, nor are they ethical from the precautionary principle. Firstly, protecting one's privacy is near impossible unless one opts out from using the internet, i.e., opts out from being a part of modern society. Secondly, by now, we know how harmful uncontrolled collecting and processing can be. Thirdly, we do not know how worse it can become.

Legislation and policies rooted in notice and choice legitimize the current treatment of personal data on the internet. Human behavior has marginally changed since notice and choice became a staple in modern privacy legislation and policies. Comparatively, the technological landscape has changed drastically in the past few decades. If privacy matters, then the regulation must shift the majority of the responsibility from the users over to the data processors. Otherwise, nothing will really change.

References

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*. 674–689.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Andersson, J., Bäck, J., & Ernbrandt, T. (2020). *Svenskarna och internet 2020* (p. 181). https://svenskarnaochinternet.se/app/uploads/2020/12/internetstiftelsen-svenskarna-och-internet-2020.pdf

Andrejevic, M. (2014). The Big Data Divide. *International Journal of Communication*, *8*, 1673–1689.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). 4. Americans' attitudes and experiences with privacy policies and laws. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

Basil, M. D. (1996). Standpoint: The Use of Student Samples in Communication Research. *Journal of Broadcasting & Electronic Media*, *40*(3), 431–440. https://doi.org/10.1080/08838159609364364

Black, I. (2013, June 10). NSA spying scandal: What we have learned. *The Guardian*. http://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned

Boerman, S. C., Kruikemeier, S., & Borgesius, F. J. Z. (2018). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, *00*(0), 25. https://doi.org/10.1177/0093650218800915

Böhme, R., & Köpsell, S. (2010). Trained to accept?: A field experiment on consent dialogs. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, 2403. https://doi.org/10.1145/1753326.1753689

boyd, danah, & Crawford, K. (2012). CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, *15*(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

Brink, H. I. L. (1993). Validity and reliability in qualitative research. *Curationis*, *16*(2), 35–38. https://doi.org/10.4102/curationis.v16i2.1396

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Carminati, L. (2018). Generalizability in Qualitative Research: A Tale of Two Traditions. *Qualitative Health Research*, *28*(13), 2094–2101. https://doi.org/10.1177/1049732318788379

Cate, F. H. (2010). The Limits of Notice and Choice. *IEEE Security & Privacy Magazine*, *8*(2), 59–62. https://doi.org/10.1109/MSP.2010.84

Cavoukian, A. (2009). *Privacy by Design, Take the Challenge*. Information and Privacy Commissioner of Ontario.

Cavoukian, A. (2011). *The 7 Foundational Principles—Implementation and Mapping of Fair Information Practices* (p. 12).

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Coenen, F. (2011). Data mining: Past, present and future. *The Knowledge Engineering Review*, *26*(1), 25–29. https://doi.org/10.1017/S0269888910000378

Custers, B., van der Hof, S., & Schermer, B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies. *Policy & Internet*, *6*(3), 268–295.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Proceedings 2019 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2019.23378

Engelmann, S., Chen, M., Fischer, F., Kao, C., & Grossklags, J. (2019). Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines "Good" and "Bad" Behavior. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 69–78. https://doi.org/10.1145/3287560.3287585

Englehardt, S., & Narayanan, A. (2016). Online Tracking: A 1-million-site Measurement and Analysis. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1388–1401. https://doi.org/10.1145/2976749.2978313

European Commission. (2016, July 5). *Cookies*. Cookies. https://ec.europa.eu/growth/cookies_en

European Data Protection Supervisor. (n.d.). *The History of the General Data Protection Regulation | European Data Protection Supervisor*. Retrieved April 7, 2021, from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Facebook. (2020, October 5). *Cookies Policy*. https://www.facebook.com/policy/cookies/printable

Floridi, L. (2010). *Information—A Very Short Introduction*. Oxford Univer.

franzke, aline shakti, Bechmann, A., Zimmer, M., Ess, C., & Association of Internet Researchers. (2020). *Internet Research: Ethical Guidelines 3.0*. https://aoir.org/reports/ethics3.pdf

Fuchs, C. (2012). Dallas Smythe Today—The Audience Commodity, the Digital Labour Debate, Marxist Political Economy and Critical Theory. Prolegomena to a Digital Labour Theory of Value. *TripleC*, *10*(2), 692–740. https://doi.org/10.1163/9789004291416

Fusch, P. I., & Ness, L. R. (2015). Are We There Yet? Data Saturation in Qualitative Research. *The Qualitative Report*, *20*(9), 1408–1416.

Gillespie, T. (2014). The Relevance of Algorithms. In T. Gillespie, P. J. Boczkowski, & K. A. Foot (Eds.), *Media Technologies* (pp. 167–194). The MIT Press. https://doi.org/10.7551/mitpress/9780262525374.003.0009

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016). How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. *Twelfth Symposium on Usable Privacy and Security (*, 321–340.

Google. (2021, February 4). *Privacy Policy*. https://policies.google.com/privacy

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Gupta, I. (2012). Are websites adequately communicating terms & conditions link in a browse-wrap agreement? *European Journal of Law and Technology*, *3*(2), 1–10.

Hare, S. (2016). For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection. *Business Horizons*, *59*(5), 549–561. https://doi.org/10.1016/j.bushor.2016.04.002

Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, *10*, 3738–3757.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me"_ Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, 1–14. https://doi.org/10.1016/j.ijhcs.2020.102498

Hu, X., & Sastry, N. (2020). What a Tangled Web We Weave: Understanding the Interconnectedness of the Third Party Cookie Ecosystem. *12th ACM Conference on Web Science*, 76–85. https://doi.org/10.1145/3394231.3397897

Integritetsskydsmyndigheten. (n.d.). *Dataskyddsförordningens syfte och tillämpningsområde*. Integritetsskyddsmyndigheten. Retrieved February 19, 2021, from https://www.imy.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningens-syfte-och-tillampningsomrade/

Internetstiftelsen. (2019). *Svenskarna och internet 2019* (p. 167). https://svenskarnaochinternet.se/app/uploads/2019/10/svenskarna-och-internet-2019-a4.pdf

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*, 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Jin, D. Y. (2021). *Political Economy of the Media*. 24.

Karlstads universitet. (2019). *Uppsatsguide—Självständiga arbeten i medie- och kommunikationsvetenskap vid Karlstads universitet*.

Keith, M. J., Lowry, P. B., Evans, C. M., & Babb, J. S. (2014). *Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure*. 19.

Kennedy, H. (2016). *Post, Mine, Repeat—Social Media Data Mining Becomes Ordinary*. Palgrave Macmillan.

Kennedy, H., Elgesem, D., & Miguel, C. (2017). On fairness: User perspectives on social media data mining. *Convergence: The International Journal of Research into New Media Technologies*, *23*(3), 270–288. https://doi.org/10.1177/1354856515592507

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018). *"This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer*. 1–11. https://dx.doi.org/10.14722/eurousec.2018.23012

Kvale, S., & Brinkmann, S. (2014). *Den kvalitativa forskningsintervjun* (3rd ed.). Studentlitteratur.

Lee, C. S. (2019). Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review*, *43*(6), 952–970. https://doi.org/10.1108/OIR-08-2018-0231

Lee, P. (2011). The impact of cookie 'consent' on targeted adverts. *Journal of Database Marketin & Customer Strategy Management*, *18*, 205–209. https://doi.org/10.1057/dbm.2011.20

Leenes, R., & Kosta, E. (2015). Taming the cookie monster with Dutch law – A tale of regulatory failure. *Computer Law & Security Review*, *31*(3), 317–335. https://doi.org/10.1016/j.clsr.2015.01.004

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure: China's Social Credit System as State Surveillance. *Policy & Internet*, *10*(4), 415–453. https://doi.org/10.1002/poi3.183

Libert, T. (2015). Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites. *International Journal of Communication*, *9*, 3544–3561.

Libert, T. (2018). An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. *Proceedings of the 2018 World Wide Web Conference on World Wide Web - WWW '18*, 207–216. https://doi.org/10.1145/3178876.3186087

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2019). The Privacy Policy Landscape After the GDPR. *ArXiv:1809.08396 [Cs]*. http://arxiv.org/abs/1809.08396

Litman-Navarro, K. (2019, June 12). Opinion | We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. *The New York Times*. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-

policies.html, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

Lucas, J. W. (2003). Theory-Testing, Generalization, and the Problem of External Validity. *Sociological Theory*, *21*(3), 236–253.

Machuletz, D., & Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), 481–498. https://doi.org/10.2478/popets-2020-0037

Mai, J.-E. (2019). Situating Personal Information: Privacy in the Algorithmic Age. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms* (pp. 95–116). The MIT Press.

Masur, P. K. (2020). How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think* (Digital). Houghton Mifflin Harcourt.

McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*, 543.

McIntosh, M. J., & Morse, J. M. (2015). Situating and Constructing Diversity in Semi-Structured Interviews. *Global Qualitative Nursing Research*, *2*, 1–12. https://doi.org/10.1177/2333393615597674

Mehrnezhad, M. (2020). A Cross-Platform Evaluation of Privacy Notices and Tracking Practices. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 97–106. https://doi.org/10.1109/EuroSPW51379.2020.00023

Messenger Davies, M., & Mosdell, N. (2006). *Practical Research Methods for Media and Cultural Studies—Making People Count*. Edinburgh University Press.

Miles, M. B., Huberman, M. A., & Saldaña, J. (2020). *Qualitative data analys: A methods sourcebook* (4th ed.). Sage. https://us.sagepub.com/sites/default/files/upm-assets/102000_book_item_102000.pdf

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, *1*(2), 13–22. https://doi.org/10.1177/160940690200100202

Mozilla. (n.d.). *Using HTTP cookies*. Retrieved April 16, 2021, from https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

Nissenbaum, H. (2010). *Privacy in Context—Technology, Policy, and the Integrity of Social Life*. Standford University Press.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Dædalus*, *140*(4), 33–48.

Nvivo. (n.d.). *NVivo Collaboration*. Retrieved May 19, 2021, from https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/about/nvivo/modules/collaboration

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

O'Reilly, M., & Parker, N. (2012). 'Unsatisfactory Saturation': A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*(2), 190–197. https://doi.org/10.1177/1468794112446106

oTranscribe. (2019, May 7). *OTranscribe Privacy Policy*. https://otranscribe.com/privacy/

Papadopoulos, E. P., Diamantaris, M., Papadopoulos, P., Petsas, T., Ioannidis, S., & Markatos, E. P. (2017). The Long-Standing Privacy Debate: Mobile Websites vs Mobile Apps. *Proceedings of the 26th International Conference on World Wide Web*, 153–162. https://doi.org/10.1145/3038912.3052691

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Peterson, R. A., & Merunka, D. R. (2014). Convenience samples of college students and research reproducibility. *Journal of Business Research*, *67*(5), 1035–1041. https://doi.org/10.1016/j.jbusres.2013.08.010

Princiya. (2019). *Lightbeam 3.0*. https://addons.mozilla.org/en-US/firefox/addon/lightbeam-3-0/

Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Reidenberg, J. R., Breaux, T., Cranor, T. F., French, B., McDonald, A., Norton, T. B., Raimanath, R., & Rjissell, N. C. (2015). *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding? 30*(1), 39–88.

Richman, W. L., Kiesler, S., Weisband, S., & Drasgow, F. (1999). A meta-analytic study of social desirability distortion in computer-administered questionnaires, traditional questionnaires, and interviews. *Journal of Applied Psychology*, *84*(5), 754–775. https://doi.org/10.1037/0021-9010.84.5.754

Rivas, C. (2015). Questions, measurement and structured observation. In C. Seale (Ed.), *Researching Society and Culture* (3rd ed., pp. 429–453). Sage.

Roosendaal, A. (2012). Massive Data Collection by Mistake? In J. Camenisch, B. Crispo, S. Fischer-Hübner, R. Leenes, & G. Russello (Eds.), *Privacy and Identity Management for Life* (Vol. 375, pp. 274–282). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-31668-5_21

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed). SAGE.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. *Proceedings*

of the 2019 ACM Asia Conference on Computer and Communications Security, 340–351. https://doi.org/10.1145/3321705.3329806

Síthigh, D. M., & Siems, M. (2019). The Chinese Social Credit System: A Model for Other Countries? *Modern Law Review*, *82*(6), 1034–1071.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Ur, B., Leon, P., Cranor, L., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. *SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security*. https://doi.org/10.1145/2335356.2335362

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990. https://doi.org/10.1145/3319535.3354212

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

van Eijk, N., Helberger, N., Kool, L., van der Plas, A., & van der Sloot, B. (2012). Online tracking: Questioning the power of informed consent. *Info*, *14*(5), 57–73. https://doi.org/10.1108/14636691211256304

van Hoboken, J. (2019). The Privacy Disconnect. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms* (pp. 255–284). The MIT Press.

Westin, A. F. (1967). *Privacy and freedom*. New York, Atheneum. http://archive.org/details/privacyfreedom00west

Wintre, M. G., North, C., & Sugar, L. A. (2001). Psychologists' response to criticisms about research based on undergraduate participants: A developmental perspective. *Canadian*

Psychology/Psychologie Candienne, *42*(3), 216–225. https://doi.org/10.1037/h0086893https://doi.org/10.1037/h0086893

Wong, K. L. X., & Dobson, A. S. (2019). We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies. *Global Media and China*, *4*(2), 220–232. https://doi.org/10.1177/2059436419856090

Appendix 1: Intervjuguide

Muntlig samtyckesblankett

Syftet med studien är att utforska hur internetanvändare värnar om sin integritet på internet.

Det är frivilligt att delta och du kan avbryta när som helst under intervjuns gång. I sådant fall behöver du inte förklara varför. Deltagandet i studien innebär att en intervju kommer genomföras via Zoom. Vi kommer spela in intervjun, både ljud och bild. All insamlad data är konfidentiella och kommer behandlas enligt dataskyddsförordningen.

Studien är det sista examinerande momentet för vår kandidatutbildning.

Introduktion

1. Berätta lite om dig själv:
    a. Hur gammal är du?
    b. Vilket program studerar du?
    c. Hur kommer det sig att du valde studera x?
2. Hur många användarkonton har du på ett ungefär som du använder regelbundet?
    a. Exempel: Google/YouTube, Blocket/Schibsted, Amazon, Spotify, etc. (Sociala medier, Snapchat, Facebook,TikTok osv.
    b. Vilka använder du mest?
3. Vilka webbsidor brukar du besöka, förutom sociala medier?
    a. Nyheter, shopping
4. Vilken/vilka enheter använder du mest när du surfar?
    a. Mobil, padda, dator, annat?
    b. Om mobil/padda - främst genom appar eller webbläsare?

Integritet på internet

5. Vilken sorts information tror du att webbsidor samlar in när du besöker dem?
6. Hur används den insamlade informationen, tror du?
7. Vilken information om dig tycker du är okej att webbsidor samlar in?
    a. Varför?
8. Vilken information om dig är oacceptabelt att webbsidor samlar in?
    a. T.ex. samtalshistorik, IP-address, email-address, enhet, geografisk positionering, sökhistorik, intressen, rörelsemönster etc.

    b. Varför?
9. Brukar du skydda din personliga integritet på internet och i sådana fall hur?
    a. Om osäker, ge förslag (adblock, don't track, VPN, inte dela visa bilder, platsinfo etc.)
10. Vem tycker du att har störst ansvar för att skydda privatpersoners integritet på internet? (
    a. Eventuellt kom med förslag om respondent är osäker?/ Som det ser ut nu är DU ansvarig för kontrollera och hantera hur webbsidor samlar in data från dig.

Samtyckesrutor

(Visa bilder på samtyckesruta/samtyckesrutor)

11. Vad brukar du göra när du ser samtyckesrutor?
12. Finns det tillfällen då du ändrar på cookieinställningarna, i sådant fall varför?
    a. Vilka inställningar ändrar du?
13. Brukar du läsa cookie-policyn när en samtyckesruta dyker upp?
    a. Om positivt: varför och hur noggrant
    b. Om negativt: Varför inte? Vad tror du skulle krävas för dig att läsa igenom den?
14. Vad tycker du är positivt med samtyckesrutor?
15. Vad tycker du är negativt med samtyckesrutor?

Visualisera trackers

Nu är vi strax klara! Men först ska visa en kort demonstration om tredjepartscookies (visa LightBeam).

16. Vad tänker du kring det vi visade?

Avrundning

17. Är det något mer du tänker kring samtyckesrutor, eller som rör något annat vi diskuterade, som vi inte har tagit upp?