17 MAY 2021

MASTER'S THESIS

DIGITAL MARKETING IN A PRIVACY-FIRST WORLD

How to prepare for the future and become a digital marketing frontrunner

AUTHORS:
AMANDA SVENDSEN (133945)
GABIJA BOGDZEVICIUTE (132507)

CHARACTERS: 171,498
PAGES: 76.85
SUPERVISOR: EDLIRA SHEHU
PROGRAMME: MSC E-BUSINESS

CBS

Abstract

The purpose of this master's thesis is to examine how businesses can prepare for an increasingly privacy-centered future. New international and local privacy regulations have forced disruption upon the digital marketing industry by heavily limiting the opportunities for collecting and utilizing data of users. Former ways of performing digital marketing practices included third-party data collected by cookies, which will become obsolete by 2022. The most dominant advertisement platforms in the industry have already stopped using tracking technologies to uniquely identify users based on browsing activities and have introduced new privacy-focused technologies as a replacement. These new technologies are researched further in this thesis to understand whether they can become an industry standard in the future. The research design for this thesis consists of mixed methods: the quantitative approach, which covers a combined online experiment and survey completed by 149 respondents, and the qualitative approach, which consists of interviews with three high-profile experts within the digital marketing industry. Seven hypotheses were tested to find out what factors would have an effect on users' intent to share their personal data. Three of the hypotheses were accepted - it was found that both personalization and privacy fatigue were proven to be negatively related to users' intent to share their personal data, whereas the value of information disclosure had a significant positive relation. The findings from this research conclude with recommendations for businesses on how to adapt to the current changes of the industry and build a future-proof strategy with a focus on user privacy. The strategy should include a comprehensive first-party data collection by delivering strong value propositions that convince users to opt-in and share their personal data.

Keywords:

Digital marketing, user privacy, personalization, first-party data, privacy-first strategy

Acknowledgements

This master's thesis was conducted with help of 149 anonymous respondents and great contributions from digital marketing experts. We would like to thank all of our respondents for taking the time to contribute to this research. A special thanks must be given to the interviewed experts: Rhys Cater, Morten Køhler Hansen, and Thomas Bering. Discussing this topic with you has been incredibly insightful and inspiring which helped us shape the recommendations presented in this thesis. Lastly, we want to thank our supervisor, Edlira Shehu, for supporting us through this journey and keeping us on the right track for this research.

Table of contents

List of tables

List of figures

1.

INTRODUCTION

PROBLEM STATEMENT

1. Introduction

At the beginning of 2020, the worldwide outbreak of COVID-19 forced people to stay home and practice social distancing. This led to higher consumption of internet services when people turned to online socializing and working from home. Subsequently, online purchases peaked across various industries. A study by the Office of National Statistics (2020) showed that especially non-store retailers (e.g. Amazon) experienced the highest growth rates ever recorded. The same study reports that over 32% of all retail businesses that sell products online experienced an increase in online sales (measured in May 2020). It is estimated that such results caused by accelerated digital transformation would have taken 10 years to take place under normal circumstances (GlobalWebIndex, 2020). Such growth of online shopping behavior puts pressure on businesses fighting to keep up with the increased demand and win market share over their competitors online. Research conducted by GlobalWebIndex (2020) states that online shopping behavior will continue to grow after overcoming the pandemic. According to their research, shopping online was the number one activity consumers said they want to keep up after the COVID-19 outbreak, and that 49% of consumers were planning to shop online more frequently compared to before the pandemic. These promising numbers made businesses across all industries invest heavier in digital marketing. Social media marketing activities alone experienced an increase of 29% in March 2020 compared to the previous quarter (Grand View Research, 2020).

Long before the COVID-19 outbreak changed the world, internet usage was increasing year on year, although the pandemic sped up the process even further. From the year 2000 to 2020, internet usage increased by 1266% (BroadBandSearch, n.d.). The worldwide rise of digital usage has naturally led to public demand for more protection of data privacy and a higher concern for companies' ethical stand regarding user data. Therefore, the world is currently moving towards a new era that involves higher levels of privacy for users, more transparency on data collection and processing, and new regulations for businesses handling personal data. As a result, former ways of tracking users will not be possible to execute anymore and third-party cookies are becoming obsolete (Bump, 2021). Apple's standard internet browser, Safari, was one of the first bigger browsers to completely block tracking by third-party cookies.

Furthermore, Google announced in March 2021 that they will stop using tracking technologies to uniquely identify users based on browsing activities as an initiative in their Privacy Sandbox project. These mentioned changes were forced upon companies due to data protection regulations and are disrupting the marketing industry entirely (ibid.).

Previously, the digital marketing industry extensively relied on cookies, while its best practices included collecting as much user data as possible (Juneau, 2020). This would often happen without users even being aware of it. Enormous data amounts were collected in Customer Relationship Management (CRM) systems to profile users, target them with specifically tailored ads, retarget them on other sites, and personalize offers based on the collected data (Kulpa, 2017). For many businesses, all these practices were heavily supported by third parties. The marketing industry is forced to change its ways of profiling users and adapt to the new international privacy regulations. New privacy standards and regulations are predicted to become a top priority for businesses and marketing agencies for the next many years to come (Warc, 2020). This can be a new era of innovation for online advertisement forcing marketers to think and act differently about data.

1.1 Problem statement

To sum up, digital marketing practices are being disrupted by (a) growing user concerns about how their data is being collected and used, (b) increasing privacy regulations, and (c) restrictive practices employed by advertising platforms and technology firms. This master's thesis researches the mentioned changes to understand what it means for users and how businesses should prepare for the future to become digital frontrunners in a privacy-first world. Thus, the research question to be answered by this thesis is the following:

How can businesses prepare for a privacy-first future to become digital marketing frontrunners?

To answer the primary research question, various sub-questions are formulated to understand the underlying problem areas.

1. *What are the current privacy trends in the digital marketing industry?*
2. *What are the factors behind the increasing demand for privacy-centered digital marketing solutions?*
3. *What are the drivers for users' willingness to share their data with companies?*

To answer these questions, an extensive literature review was conducted to examine previous findings from similar research areas, which lead to the formulation of hypotheses to be tested by a combined quantitative online experiment and survey. This research is based on mixed methods, whereas the quantitative results were analyzed and hereafter discussed in qualitative interviews with high-profile experts within the field of digital marketing. The expert interviews further entailed a discussion on the current privacy-focused industry trends and their experiences within the field of digital marketing. These steps resulted in various findings used to formulate advice for businesses to prepare for a privacy-focused future.

2.

CONTEXTUAL BACKGROUND

PRIVACY LEGISLATION, TECHNICAL DESCRIPTIONS, INDUSTRY PRIVACY-FOCUSED TRENDS

2. Contextual background

Before this research can be presented, a contextual background is provided to establish the timeline of the mentioned changes and the reasoning for their enforcement. This chapter helps the reader understand the basis for the research. Firstly, the chapter covers the legal foundation for the changes that were demanded upon the industry. Secondly, a definition of cookies, pixels, and first-party data is provided to establish a common ground for discussing these terms later on. Lastly, various industry trends are presented to understand the themes that are discussed later in this report with the digital marketing experts.

2.1 Privacy legislation

The following sections cover the newly adopted legislation regarding data privacy from a European and American perspective. This forms the foundation of understanding the reasoning behind these worldwide changes that have an impact on businesses currently.

2.1.1 General Data Protection Regulation (GDPR)

The European Union enforced a new General Data Protection Regulation in 2018, replacing the former EU Data Protection Directive from 1995 (European Commission, n.d.). According to the European Commission, the data protection regulation aims at making Europe fit for the digital age (ibid.). Being a regulation rather than a directive ensures that every member state of the European Union applies this common standard and replaces the different national data protection laws. The purpose of this regulation is to secure consumer's online rights, strengthen the security standards for data privacy, and force companies to treat personal data with respect (ibid.). With new standards for collecting, handling, and sharing consumer data, privacy has become a top priority when designing new services. The regulation secures consumers' rights and requires consumer content to be explicit and opt-in, rather than opt-out. As an example, consumers can only legally allow cookie-tracking by opt-in instead of opt-out (the strictly necessary cookies are an exception to this rule, e.g. for completing a purchase). This will be described further in the following sections.

2.1.2 ePrivacy Directive

While the GDPR focuses more on general data privacy, the Electronic Privacy Directive (EPD) goes into more technical details. As an example, the GDPR only mentions cookies once, in Recital 30, while EPD also goes under the alias “the cookie law” since its most notable effect was the proliferation of cookie consent pop-ups (Koch, 2019). The EPD is considered a supplement to the GDPR, addressing crucial aspects to electronic communications and tracking of Internet users. Eventually, the EPD will be replaced with the ePrivacy Regulation (EPR) which builds on top of the EPD and expands its definitions. Regulation within the EU becomes legally binding throughout the EU starting from the date it comes into effect. A directive, however, is only required to be incorporated into the national laws of the member states, allowing member states to make changes to adapt to their own wishes. The implementation of the EPR will be more comprehensive than the EPD which addresses browser fingerprinting in ways that are similar to cookies and creates more robust protection of metadata. The EPR was planned to be passed in 2018 along with the GDPR but has been stuck in the approval process for some years. It is expected that the EPR will be passed during 2021 (Sippel, 2021).

2.1.3 Local legislation concerning data privacy

Outside of the European Union (EU), countries and states have been formulating their own versions of a general data privacy regulation. One thing most of these regulations have in common is that they were heavily inspired by the EU’s GDPR. The GDPR is a common standard to build legislation from and has been kick-starting the privacy debate all over the globe.

One example of local legislation concerning data privacy is the California Consumer Privacy Act (CCPA), implemented on the 1st of January 2020 (Ramirez, 2020). The CCPA contains many similar elements to the GDPR, including the right to opt-out of the collecting of personal data. The CCPA also has extra protection which is not included in the GDPR, e.g. it gives consumers the ability to stop a company from selling their personal data (ibid.). The CCPA applies to for-profit organizations where 50% of the revenue comes from selling

consumer data, the annual revenue is above $25 million, and has data collected related to at least 50,000 Californians. Breaches of the CCPA may result in fines up to $7,500 for intentional violations (Digital Information World, 2020).

Many other countries have implemented their own version of the GDPR. To name a few, Australia has its Privacy Amendment from 2018, Brazil implemented their Lei Geral de Proteção de Dados (LGPD) in February 2020, India has introduced a Personal Data Protection Bill (PDPB), and China is working on a Personal Data Protection Law (PDPL) (Simmons, 2021).

2.2 Technical descriptions

The following sections explain the technical details of subjects that will be discussed later in this thesis. Technical descriptions of cookies, pixels, third-party cookies, and first-party data will be provided to form the foundation for understanding future findings.

2.2.1 Cookies and pixels

A cookie is a small piece of code (also known as script) stored in the internet browser of the visitor (TechTerms, 2011). The purpose behind the implementation of cookies is to remember the user's activity and preferences for future usage, improving the user experience, and profiling for marketing initiatives. Cookies can have many qualities e.g. storing user log-in information and connecting the user to a segmentation. Some cookies are necessary for a website to implement and do not require a legal basis for opt-in as the majority of cookies need. An example of a necessary cookie within an e-commerce site is the cookie storing data regarding a product added to the shopping cart to proceed with a purchase. This cookie is known as a 'session cookie' and will be deleted when the user leaves the website.

Other cookies are known as 'persistent cookies' since they also operate and function after a user exits the website. These cookies cover the previously mentioned qualities of storing log-in, remembering user preferences, customer segmentation, etc. The expiration of these cookies can be programmed to be whenever the programmer wants them to be. Cookies only

recognize the user when he/she is operating the same internet browser since the code is stored in the browser. When the user is moving to another device, a pixel can be a way of tracking and recognizing the user on multiple devices and connecting the information from different sources (ibid).

Pixels used for tracking cross-device are an effective way of profiling users. Not to be confused with the pixels used for displaying images in digital photography. Tracking pixels are built similar to cookies, which means that they also consist of a code snippet. The code shows as a tiny 1x1 pixel graphic on the website, so small it is impossible for the user to see. This code can be added to a particular website, e.g. the Facebook Pixel is added to almost every webshop by the website owners. The Facebook pixel can currently be used for tracking both 1st party and 3rd party cookies. They are primarily used for retargeting purposes and thereby improving conversion rates. The main difference between cookies and pixels is where they are stored: cookies are stored in a particular browser, pixels are stored by websites. Cookies can be cleared or even blocked entirely by users if they go to their browser settings, but pixels cannot be cleared or blocked the same way by users. The user can visit another website with a pixel installed and the pixel continues to collect information about the user's preferences and online habits (AdQuadrant, 2020). The pixel is known for being more accurate when tracking users across multiple devices. As an example with the Facebook pixel, the users are often signed in to Facebook on every device they may own and the pixel can thereby track a particular user across multiple devices. If one were to rely solely on cookies connected to an analytics software as the only data source, the analytics software would often count every visit from each device as a new person.

2.2.2 Third-party cookies

Digital marketing as we know it will be disrupted once restrictions of cookie-tracking will be enforced. The internet browsers, Safari and Firefox, have already outfaced third-party cookie tracking and Google Chrome is moving towards outfacing by the end of 2022 (Bump, 2021). Third-party cookies have been utilized in broad ways of audience targeting and remarketing

practices. They have been important when tracking users across different channels and provide companies with very accurate personalization possibilities.

Although third-party cookies sound like an effective way of tracking, they do have some limitations. This includes questionable data quality, limited scale, and compliance issues. The questionable data quality often stems from cookies being 60-90 days old. This gives a flawed version of a user's current behavior and needs. As an example, a user could be searching for a new bike to buy, find one to purchase, and still receive ads related to bikes months after. Another reason for the declining data quality is the rising usage of ad-blockers installed by users and the rising amount of users of the internet browser, Safari (currently being the standard browser for 19% of the world's population), which has a high defense for tracking technologies (StatCounter, 2021). Ad-blockers are used by 40% of European internet users and prevent tracking through third-party cookies since there is no script for them to track. Established enterprises have already built their own databases/CRM systems to manage customers and leads. A newly established business with a humble data collection will face difficulties when targeting potential customers after Google shuts down the possibility for sharing third-party data. Bigger companies are not relying as much on this technology and will therefore not be as vulnerable to this change compared to small and medium sized businesses. Since third-party data is becoming less relevant and is currently being outfaced, first-party data is often preferred by businesses for more accurate targeting.

2.2.3 First-party data

Without the possibility of utilizing cookies, businesses will be forced to pivot toward evolving their own technology, becoming better at collecting first-party data, and performing contextual targeting. First-party data is defined as data companies collect directly from their consumers, including information about purchase intention, browsing behavior on the company's website/app, transaction history from the company's CRM-database, loyalty program activity, and general information regarding the user's preferences (Boston Consulting Group, 2020).

The goal for businesses is to collect accurate and relevant first-party data to create strong value from personalization principles. Businesses who leverage data-driven personalization techniques well will experience a gain of 5-8 times return on investment (ROI) on their marketing spend (Rudolph, 2018). According to Google, 90% of marketers say that first-party data is important to their digital marketing strategies. The same study shows that only 30% of these marketers are collecting and integrating data across channels and only 1% are using data to deliver a fully cross-channel experience for their customers (Boston Consulting Group, 2020). While it is a common understanding in the industry that leveraging first-party data is highly important to future-proof a business, many companies struggle to find a way to collect and use first-party data on a larger scale.

Companies are highly focused on collecting and utilizing data from consumers to create better products and services, but consumers are currently more resistant to sharing their personal data. Although, research has shown that 61% of Americans are willing to share their personal data to receive personalized marketing communications. This indicates that the consumers might be willing to expose their personal data if the value in return is good enough. This number is high compared to UK citizens where 48% agree to this trade-off (Koetsier, 2018). Trust has appeared to be a very important element when users decide whether they will share their data with a business. Customers are much more likely to share their data with companies that actively work to generate trust. Another important factor to determine the willingness of data sharing from users is value creation. This factor is intertwined with trust since the more value a company offers, the more trust they earn with the customer. It is crucial for businesses to keep improving their customer trust and value creation in exchange for data because consumers can easily opt out and withdraw their permission if they no longer trust the company or if the benefits are not sufficient enough (Boston Consulting Group, 2020).

2.3 Industry privacy-focused trends

Businesses all over the world have met challenges trying to keep up with the rising demand for data privacy and more transparency. Popular Netflix documentaries, such as The Social

Dilemma (2020), have made consumers more aware of how they are being exploited just by browsing on websites online. Tech companies have been forced to innovate their ways of tracking users and have developed new technology to replace individual tracking. Many different techniques have been widely discussed in the media landscape. The following sections cover the biggest privacy-focused industry trends and what changes they may bring to the digital marketing industry.

2.3.1 Differential privacy

Differential privacy is a technique used for securing the privacy of data subjects when analyzing large datasets. The technique was invented by Microsoft researchers in 2016, and since then, differentially private algorithms have been adopted by many of the biggest tech companies: Apple, Facebook, Google, Uber, Amazon, Snapchat, Salesforce, etc. (Schiff, 2020). The purpose of differential privacy is to eliminate the risk of reverse-engineering sensitive data while still maintaining the possibility of analyzing and utilizing the data. This way it can be possible to spot trends from data without the possibility of identifying the data subject. This technique goes beyond just anonymizing data since a collection of different data sources would make it possible to identify a person. Instead, differentially private algorithms are adding random noise to the dataset making it imprecise and (almost) impossible to identify the data subjects. A Privacy Tool project by Harvard University explains: “The guarantee of a differentially private algorithm is that its behavior hardly changes when a single individual joins or leaves the dataset — anything the algorithm might output on a database containing some individual’s information is almost as likely to have come from a database without that individual’s information. … This gives a formal guarantee that individual-level information about participants in the database is not leaked.” (Harvard University, n.d.).

As an example of why differential privacy is important: Netflix released a dataset in 2007 of their user ratings as part of a competition to see if anyone could outperform their own filtering algorithm. The data was anonymous, but some competitors succeeded in identifying the data subjects anyway. They identified 99% of the personal information by comparing

Netflix's data to IMDB's data. This incident showed that if an entity holds enough data from multiple sources, anyone can, in theory, be identified even though the data was anonymized originally. Therefore, the differential privacy technique can be a very useful solution to this problem when dealing with sensitive data and for securing the anonymity of data subjects so they cannot be identified in any way (Medium, 2018).

2.3.2 FLoC Technology

Related to differential privacy, a privacy-preserving machine learning mechanism named The Federated Learning of Cohorts (FLoC) has been developed by Google for their Privacy Sandbox project and was introduced on January 14, 2020. FLoC is planned to replace cookies when third-party cookies will be phased out from the Google Chrome browser in 2022. The technology divides users who express similar interests from their browsing activities into *cohorts*, a segmentation group similar to what previously has been done through cookies. The way it differs from cookie-tracking is how they hide users in crowds of a minimum of a thousand other users, and the web history is kept in the browser instead of being uploaded anywhere for a third party to leverage. Instead of targeting individual users from their user ID, FLoC works by targeting the cohort ID. Therefore, the individual user will no longer be tracked across their paths on the internet nor have personal information revealed. Instead, the user is grouped into cohorts of similar people. According to Google, a cohort ID can be differentially private and still be used as a digital fingerprint. Google is relying on the FLoC technology and says it will deliver results nearly as effective as cookie-based approaches: "Our tests of FLoC to reach in-market and affinity Google Audiences show that advertisers can expect to see at least 95% of the conversions per dollar spent when compared to cookie-based advertising" (Bindra, 2021).

However, FLoC-technology is faced with some critique from the industry. It is still a tracking solution that could potentially involve sensitive personal data related to users. It is also a concern to some whether there is a possibility that a person can be identified by tying data together from multiple sources as explained in the previous section on differential privacy.

FLoC is considered an improvement from previous cookie-based tracking in terms of privacy, but not a perfect bulletproof solution yet (Davis, 2021).

2.3.3 Privacy-first internet browsers

A new demand for privacy-focused internet browsers has been rising during the last couple of years. Furthermore, new privacy legislation has put pressure on the most popular internet browsers and forced them to apply changes to their way of tracking their users. Mozilla's Firefox is one example of a browser that has upgraded its privacy standards for users recently. Firefox claims to collect a minimum of data and blocks trackers by default. Another example of an improved internet browser on the privacy scene is Safari, the default browser of Apple's devices. With their new updates to the Safari browser, cross-site tracking has been blocked and their Intelligent Tracking Prevention (ITP) has evolved even stronger by reducing the lifespan of tracking cookies to 7 days (InterestExplorer, n.d.).

Even though the mentioned internet browsers have been willing to adapt to new privacy demands and many have applied the changes before they were due, consumers still express a lack of trust towards these tech giants behind the browsers. As an alternative, a new free internet browser, Brave, has been introduced to the market in 2016. Brave is considered one of the absolute most private browsers on the market and they can ensure 3 times faster browsing experience compared to competitors by blocking ads. One of Brave's co-founders, Brendan Eich, is the creator behind Javascript and was kick-starting Firefox back in the days (Keizer, 2021). Brave neither detects nor stores the users browsing activities and can therefore never be sold to a third party. This will naturally become an issue for marketers, as Brave already has 25 million monthly users and is currently still growing rapidly. Although, the browser does entail one opportunity for displaying ads if the user allows it. By allowing ads displayed in the browser, the user will earn credit from a virtual currency which can be donated to the user's preferred websites whom they wish to support. The ads are not individually targeted, but aimed at anonymous aggregated data from the browser's user base (ibid.).

2.3.4 App Tracking Transparency

Apple has been a privacy frontrunner for several years and recently implemented App Tracking Transparency (ATT) in their iOS 14.5 update which eliminated the opportunity for apps to track users without explicit permission. Previously with iOS 13 and every former operating system for Apple devices, Identifier for Advertisers (IDFA) tracking was activated for all users by default. The user could opt-out of this by changing their settings. With the new iOS 14.5 update that was rolled out at the end of April 2021, IDFA tracking is only possible to utilize if the user explicitly consents to it which only 4-12% of users are currently willing to (Kraus, 2021). This change will strengthen the user privacy and Apple's privacy-concerned branding but limit attribution for marketers. The IDFA was helpful for mobile marketers when attributing their ad spend. As an example, when running user acquisition campaigns to gain new mobile customers, the IDFA tracked whether an app install was performed or if any purchase has been made after a click on the ad. IDFA has been very useful for evaluating the results of any particular marketing effort and finding similar customers. To quantify the impact this iOS update has on mobile marketing, it is estimated that mobile app install spend is around $80 billion in 2020 and has grown even bigger after the COVID-19 outbreak where mobile usage has increased rapidly. After IDFA tracking has been heavily limited, it will be a challenge for marketers to evaluate their campaigns and effectively measure the performance of their ads.

Apple has been met with extreme criticism from tech companies and the marketing industry after applying these changes to IDFA. Facebook has been the most vocal at opposing Apple's move – Facebook founder and CEO Mark Zuckerberg has stated that Apple is exploiting its "dominant platform position" (Morrison, 2021). One of the main arguments from Facebook's side is that the system update will have a negative impact on small businesses that rely on tracking and targeting technologies offered by the big platforms (Kafka & Morrison, 2021) and that have limited digital marketing budgets, thus such move would significantly impact their return on ad investment (Federighi & Stern, 2021). However, experts are critical of how influential the iOS update will be for the big advertising platforms such as Facebook and Google since they still have significant leverage over the amount of user data being generated on their own platforms (Lewellyn & Mims, 2021). Such move from Apple's side could be

driven by two main potential motivations: (1) to position themselves as privacy frontrunners in the eyes of consumers; (2) to distinguish themselves from other major technology companies such as Facebook and Google in the eyes of regulators (Kafka & Morrison, 2021).

To accommodate the need for a solution, Apple has announced that they are currently developing a privacy-focused alternative to IDFA called SKAdNetwork. This alternative will help advertisers measure the performance of their ad campaigns while maintaining the user's privacy and does not require user consent (Apple Developer, n.d.). SKAdNetwork will show the advertiser which ad resulted in the desired action without revealing which device or user initiated this. The connection is handled through cryptographically signed notifications to an ad network (Koetsier, 2020). While this could sound promising, the opportunity for targeting look-alike audiences or retargeting users with ads will not be possible to perform with SKAdNetwork as this requires information regarding the specific device or user. The SKAdNetwork will be a very limited version of the IDFA when it comes to tracking (Koetsier, 2021).

3.

LITERATURE REVIEW

THE TRANSFORMING WEB, USER APPROACH TO PRIVACY TRADE-OFF

3. Literature review

This chapter identifies and explains the most relevant and significant research related to the current state of the internet, digital marketing, data privacy, personalization, and other relevant phenomena. The discussed research articles were used to formulate the variables and hypotheses that are later tested in the analysis. The literature review serves as the foundation of this research providing a comprehensive understanding of this thesis topic.

3.1 The transforming Web

One of the main inspirations for this thesis was a research paper by Thomaz et al. (2020) who argued that the current nature of the internet is shifting towards the nature of the Dark Web due to information sharing and privacy practices. The authors state that over the next five years the shift will be apparent - firms will lose their ability to fuel current modern marketing machinery, dependent on abundant, timely, and rich consumer data.

Yadav and Pavlou (2019) state that the main change happening currently and influencing the future of both physical and online environments is not just technology but technology-enabled interactions between the key marketplace entities - consumers and firms. The authors describe a few significant trends that affect various industries, however, the most relevant ones for this thesis are *artificial intelligence* (AI) and *digital consumer orientation*. AI technologies will evolve from analyzing numerical data to becoming better at textual and contextual data such as images (Yadav & Pavlou, 2019). It will enable advertising platforms and marketers to automatically collect and process a broader scope of content to draw insights about consumers. Davenport et al. (2020) expand on the topic of modern AI, saying that today the combination of AI and big data implies that firms know much about their customers, however, currently, the technology is deployed in ways that augment rather than replace human managers. The authors note that AI raises numerous concerns for consumers who worry about the privacy of their data: the low cost of storage implies that data may exist substantially longer than intended, data may be repackaged and reused for rationales different

than those intended, and data for a certain individual may contain information about other individuals.

Another trend is researched by Kopalle et al. (2019), who has investigated the concept named *digital consumer orientation* which describes a collection of real-time data during the consumption process that the user is involved in and then using this data to optimize value delivery. However, for such real-time suggestions to work, it is still important what data consumers are willing to provide. As an example, when riding Uber some information is collected automatically (such as starting time and place of an itinerary), however, the collection of other types of information (e.g. a customer's subjective perception of how a ride is progressing) depends on a customer's willingness to share. The more data users share the better optimized value firms can offer. Yadav and Pavlou (2019) sum up these trends stating that moving forward all marketplace entities will have to adapt to the societal, legal, economic, policy, and ethical implications of increasingly automated firm-consumer interactions driven by technology.

There are a couple of phenomenons that are particularly relevant in the era of the transforming web and this thesis. Firstly, it is a *personalization privacy paradox*, that represents the discrepancies between user attitude and their actual behavior, which contrasts the assumption that privacy-related decision making is only rational (Norberg, Horne, & Horne, 2007). Xu et al. (2011), explain that personalization is dependent on consumers sharing their private information, however, consumers might be willing to give out as little information as possible even if they value personalization or expect to receive personalization benefits. Thomaz et al. (2020) state that firms adapting to the new web environment will need to understand how they are affected by the personalization privacy paradox and which consumer-oriented technologies will generate the greatest value for consumers in a way to tip the trade-off towards data sharing. Davenport et al. (2020) also agree that consumers have to balance privacy concerns against the benefits of personalized information and offers. The authors wonder how consumers determine the optimal trade-off. They also raise a few questions on whether the trade-off depends on the product category or the level of the customer's trust in the firm and if this trade-off would shift over time.

Secondly, the phenomenon of *privacy fatigue* is particularly interesting and prevalent even though it is less empirically researched by scholars than the *personalization-privacy paradox*. The phenomenon refers to the exhaustion and cynicism related to managing one's privacy and has shown to have a strong influence on privacy-related behavior (Choi et al., 2018). Privacy fatigue emerged due to the increasing difficulty in managing one's personal data and feelings of loss of control (Choi et al., 2018). Choi et al. (2018) found that privacy fatigue, particularly emotional exhaustion and cynicism dimensions, has a stronger impact on privacy behavior than privacy concerns do. According to the authors, it can potentially have a long-term impact on online vendors and policymakers. Online vendors can use the information consumers disclose to offer value-added benefits, however, if privacy fatigue is prevalent among users, the value of personal information decreases and leads to decreased user engagement to provide the information. Choi et al. (2018) suggest that policymakers should continue discussing privacy issues from the viewpoint of users to create policies that meet an acceptable level of privacy protection thus combating privacy fatigue.

3.2 User approach to privacy trade-off

"Data is the new gold. It's the new oil. It's the new plastics." (Cuban, 2017). The popular quote accurately represents the importance of user data for today's businesses, especially for web and marketing-related practices. Companies are competing for this "new gold", while legislators are trying to bring order and protect users' interests. In the following sections, it is analyzed what the user standpoint and perceptions are in the era of the transforming web.

3.2.1 User perceptions on privacy

Thomaz et al. (2020) argue that in the era of the transformed web, which has elements of the Dark Web, users can be divided into two types:

1) those willing to share their data with marketers (buffs)
2) those who deny access to their personal information (ghosts)

Karwatzki et al. (2017) state that in relation to the personalization-privacy paradox, individuals' privacy valuation is a strong inhibitor of information provision in general. Quinn (2016) has identified how specific areas of privacy concern relate to levels of individual privacy regulation offering new insight into the personalization-privacy paradox, including motivations behind sharing private data. The researcher identified that concerns about privacy revolve around four main areas: power loss (concerns about the misuse of information by those holding power), identity loss (includes deception and identity theft), future of life (future use of information to judge the individual) and information control (unwanted others accessing sensitive information). The study identified that identity loss and future of life are the main privacy concern dimensions in a social media context. Users concerned about information control and the future of life tend to address these concerns by engaging with application-level controls, while sophisticated measures, such as encryption and privacy plug-ins, are used in response to concerns about power and identity loss.

Distler et al. (2020) define privacy as an individual's ability to maintain control of their personal information. The authors recognize that privacy initiatives such as GDPR in the European Union among other measures establish the principle of *privacy by design*, which is an approach that seeks to ensure protection for the privacy of individuals by integrating considerations of privacy issues from the very beginning of the development of products or services and can be contrasted to an alternative process where privacy implications are not considered until just before launch (Kubo et al., 2019). They state that in spite of privacy and security breaches becoming common nowadays, users still often compromise their privacy in exchange for benefits of technology or service. In the context of technologies, users' privacy behavior reflects both conscious and unconscious decisions on whether they accept privacy trade-offs, such as sharing personal information (Rainie & Duggan, 2015). Users get involved in the trade-off if they believe that they will get a certain value in return (Rainie & Duggan, 2015). Sanchez et al. (2019) have also investigated the value of information disclosure and found supporting evidence that users' decisions tend to depend on the risks and benefits of disclosure. Moreover, the authors state that users' preferences are rarely static, meaning that the preferences can evolve and call it *users' preference dynamics*. Lastly, Sanchez et al. (2019) found that users' privacy settings can be predicted depending on user traits.

In addition, Distler et al. (2020) found that users' intent to disclose personal data depends on how *private* or *sensitive* the type of data shared was perceived by the research participants, while they often appreciated transparency on what kind of data is being collected. Distler et al. (2020) discussed a theory of *privacy calculus*, which measures people's intention to disclose personal information based on their goal to maximize the positive and minimize the negative consequences (Wottrich, van Reijmersdal, & Smit, 2018). The model has been used in various contexts such as social networks, mobile devices, and e-commerce (Distler et al, 2020).

Lastly, Bietz et al. (2019) found that sensitivity towards sharing private information depends on the age of users. Young adults rated lower on various health information sensitivities than researched adults. Young adults feel that they can control their personal information and feel comfortable with employing privacy-protecting strategies. Their awareness of personal information collection is higher and they are less likely to see it as a violation. It does not mean that young adults care less about privacy - the study suggests that they simply perceive certain types of information collection as less threatening compared to older age groups.

3.2.2 Personalization

Thomaz et al. (2020) state that the best option to get data from users is to encourage them to exchange it for hyper-personalization. As an example of a tool that could provide high-level personalization, researchers discuss the adoption of *conversational assistants* - chatbots. Other researches discussed in this literature review also recognize that opt-in can be achieved by exchanging value for user data while personalization is one of the most commonly suggested remunerations.

Sheng et al. (2008) discuss the ubiquitous commerce (u-commerce) adoption, which researchers consider to be the ultimate form of commerce, where users can interact and transact anywhere, anytime with anyone (e.g. users can buy concert tickets by scanning a QR code on a physical promotional poster). The idea of u-commerce is relevant for the topic

since personalization is the key for it to work. U-commerce employs technologies such as Global Positioning System (GPS), Radio Frequency Identification (RFID), and sensor network that have the ability to identify, track, and trace objects automatically making it possible to personalize offerings based on users' location and identities. The authors recognize that a higher degree of personalization brings benefits to the customers, however, it also affects privacy concerns. This statement is also supported by Cheng and Jiang (2020) who found that when users are exposed to the benefits of personalization their concerns about the amount of collected personal information increases.

Some research supports the value of personalization in advertising specifically. Walrave et al. (2018) found that highly personalized ads were preferred among adolescents, even though authors expected privacy concerns to appear in the form of personalization resistance. It proposes evidence that the benefits from sharing privacy-sensitive information might outweigh the disadvantages. Xu et al. (2011) extend the previously discussed privacy calculus discussion and distinguish two types of personalization mechanisms - covert and overt. Using the convert-based approach, marketers deliver relevant value offerings to users by secretly observing user behavior, e.g. through tracking physical locations of their mobile devices and tailoring ads to the known proximity. In contrast, the overt approach requires action initiated by the user, e.g. in the location-aware-marketing a user would signal a service provider for specific information or service such as coupons to the nearest store. Thus, users exercise greater control over the interaction in the overt approach. The results of the study suggest that the influence of personalization on the perceived risks and benefits of privacy vary depending on the type of personalization and that personal characteristics moderate the effects on the privacy calculus model (Xu et al., 2011). Furthermore, researchers found that personalization can override concerns for both covert and overt marketing efforts in a location-aware marketing context. Consumers' value for personalization was almost twice as influential as their concerns for privacy.

On the other hand, there are researchers who do not believe that personalization is beneficial in every context or have even discovered negative effects of personalization overall. Zhang et al. (2014) describe the exchange between privacy and personalization as a substitution

relationship or negative synergy. Karwatzki et al. (2017) argue that personalization benefits only convince consumers who exhibit little focus on privacy. Sheng et al. (2008) found that user's privacy concerns and perceived value of personalization vary according to the situation and context. The difference in customers' privacy concerns between non-personalization and personalization is greater in a non-emergency than in an emergency context. Emergency contexts are three-dimensional. They are represented by situations that are time-critical, location important, and where user identity is needed. Emergency context could also be explained as potentially harmful to the human whether that is a minor incident as getting lost in an unfamiliar location or major risks such as natural disasters (Sheng et al., 2008). Adding to the importance of the context, Martin and Shilton (2016) found that when making judgments about privacy, users with less experience in a context rely more on individual preferences such as generalized privacy beliefs, while users that are more experienced in the context are influenced by contextual factors and norms. In such a way, authors draw a connection between an individual's general privacy attitudes and nuanced contextual factors.

3.2.3 Information transparency

Information transparency is another important factor when evaluating users' willingness to share their personal information. Awad and Krishnan (2006) found that users who value greater information transparency are less willing to be profiled (or in other words are less willing to provide personal information). Marketers should find this puzzling since users who value information transparency features are also the consumers that are less willing to share their data. Authors suggest firms adopt a strategy of providing features that address the needs of consumers who value personalization and are willing to share some data in exchange, therefore accepting that the privacy-sensitive minority of consumers are unwilling to participate in personalization, despite additional privacy features. According to Thomaz et al. (2020), personal information disclosure can be encouraged when firms provide assurances of algorithmic fairness and transparency. Fairness means being treated without bias such as race, gender, or economic status, while transparency is firms' willingness to share how the information about users has been derived. Thomaz et al. (2020) state that ask-but-explain-why transparency can mitigate feelings of vulnerability and incentivize Ghost consumers to

share their personal data. Supporting the described findings and using the context of cookie opt-in, Miyazaki (2008) found that consumers' negative reactions to cookie use are significantly reduced by a priori cookie disclosure by the visited website promoting the benefits of information transparency. However, in contrast, Katwatzki et al. (2017) conducted a study which surprisingly found no indication that providing transparency features facilitates individuals' information disclosure.

3.2.4 Hedonic and utilitarian features

Although people state that they are concerned about their privacy, users engage in online behaviors that are contrary to this stated belief that might be encouraged by various hedonic and utilitarian value propositions (Church et al., 2017). Shobeiri et al. (2014) sum up a variety of website features into hedonic (intrinsic) and utilitarian (extrinsic). Richard (2005) explains hedonic features as low task-relevant (mainly entertainment), while utilitarian features are high task-relevant (structure, organization, informativeness, effectiveness, and navigational characteristics). Church et al. (2017) explain hedonic features as providing self-fulfillment and fun, thereby encouraging prolonged use of the product or service rather than productive use, which would be encouraged by utilitarian features. Shobeiri et al. (2014) compare extrinsic and intrinsic values when investigating how experiential values offered by an online store can improve user involvement. Researchers state that both utilitarian and hedonic elements of the website are important and engaging. However, they found that extrinsic values, specifically service excellence and customer return on investment, are more important than intrinsic values, such as aesthetics and playfulness. Moreover, as consumer's shopping experience increases, so does the need for efficiency that allows accomplishing the task, while hedonic aspects of the website become less relevant. The importance of context in terms of task experience is in line with previously mentioned research, such as Miyazaki (2008), who states that consumers' online experience and desire for privacy act as moderators of reactions to cookies used by a website. Distler et al. (2020) also researched how hedonic and utilitarian (in their words pragmatic) factors play a role when users evaluate the acceptability of privacy tradeoffs. They found that pragmatic factors such as perceived usefulness were crucial, while hedonic qualities, such as psychological needs for autonomy

and control had a strong influence on the perceived acceptability. Lastly, Church et al. (2017) found that hedonic benefits, especially enjoyment, incentivizes users to ignore privacy concerns, while Gan and Li (2018) found that perceived enjoyment has a strong effect on the intention to continuously use a service.

The previously mentioned study conducted by Quinn (2016) identified the importance of gratification when engaging users and making them trade privacy for certain social goals. The research focused on user involvement with social media platforms and identified nine uses of gratification: affect, companionship, voyeur, information sharing, habit, entertainment, communication, personal use and escape. These gratification elements are related to privacy concern dimensions discussed previously (power loss, identity loss, future of life, and information control). As an example, using social media to find out about others (voyeur gratification) is strongly associated with concerns related to identity loss and future life of information, while habit is related to lack of engagement with privacy management tools. Nine gratifications could be attributed to hedonic or utilitarian value categories suggested by Shobeiri et al. (2014), Church et al. (2017), and Gan and Li (2018): affect, companionship, voyeur, entertainment, and escape could be interpreted as hedonic gratifications, while information sharing, communication, and personal use could fall under utilitarian gratifications. Cheng and Jiang (2020) also researched how utilitarian (information) and hedonic (entertainment) gratifications impact user experience and perceived privacy risk in an artificial intelligence-driven chatbots context. They found that both utilitarian and hedonic gratifications positively affect user satisfaction with chatbot services, while perceived privacy risk reduced user satisfaction.

The main topics derived from the reviewed literature are summed up in table 1. It is also indicated which authors have researched these topics and what methods they used.

Table 1

Literature review matrix

Authors	Methodology	Intent to disclose personal information	Personalization	Hedonic features	Utilitarian features	Transparency	Value of information disclosure	General privacy concerns	Privacy fatigue
Thomaz et al. (2020)	Conceptual literature research	x	x			x		x	
Zhang et. al (2014)	Survey	x	x						
Walrave et al. (2018)	Experiment	x	x						
Awad & Krishnan (2006)	Survey	x	x			x	x	x	
Sheng et al. (2008)	Experiment	x	x						
Karwatzki et al. (2017)	Experiment	x	x			x			
Shobeiri et al. (2014)	Survey	x		x	x				
Miyazaki (2008)	Experiment	x				x			
Quinn (2016)	Survey	x		x	x				
Distler et al. (2020)	Focus group interviews	x		x	x		x	x	x
Cheng & Jiang (2020)	Survey	x	x	x	x			x	
Gan & Li (2018)	Survey	x		x	x				
Xu et al. (2011)	Experiment	x	x					x	
Choi et al. (2018)	Survey	x					x	x	x
Sanchez et al. (2019)	Survey	x	x				x	x	
Church et al. (2017)	Survey	x		x	x		x	x	

All in all, the literature review draws attention to various aspects that influence consumers' willingness to share their private data but it has not caught up yet with such a rapid development of the privacy phenomenon in the field of digital marketing. This research is contributing to the field by finding out what prerequisites have to be in place for users to be willing to share their private data and connecting it to the current and anticipated trends in the digital marketing and privacy area. Moreover, this research encompasses the perspective of various stakeholders - users, businesses, agencies, and advertising platforms - who all have different incentives when participating in the current digital marketing environment thus creating a more comprehensive view of the problem.

4.

RESEARCH THEORETICAL AND CONCEPTUAL FRAMEWORK

VARIABLES, HYPOTHESES

4. Research theoretical and conceptual framework

In this section, it is explained what variables were distinguished for the analysis. These variables and the insights drawn from the literature review were used to formulate hypotheses and to visually represent the research conceptual framework.

4.1 Variables

Based on the literature review we identified the dependent variable and two groups of independent variables used for constructing hypotheses and conceptual framework for the quantitative research part.

First, each author reviewed in the literature analysis discussed privacy and more specifically consumer *intent to disclose personal information*. Thus, this was chosen as a dependent variable. Consumer intent to disclose personal information is and will be increasingly relevant in the future of digital marketing where users are likely to have more control over their personal data and more options to choose how they want to manage it and with whom to share it.

Additionally, four independent variables were defined that serve as potential value offerings that could be traded for providing personal information or, in other words, as privacy trade-offs. The *personalization variable* in this context represents a value offering that is designed to meet the user's individual needs. As an opposite to personalization, we also introduced a *non-personalization* or generic variable that represents value offering that is not tailored to anyone individually. This was done to be able to measure the *personalization variable* more effectively by comparing its effect on the *intention to disclose personal information* to *non-personalization*. Another variable named *hedonic value offering* represents enjoyment as opposed to *utilitarian value offering*, which represents users' monetary gains and is rather pragmatic. The group of variables was named *content of value offerings*.

Lastly, the reviewed literature showcased that there are variables, which explain *user perceptions* rather than the *content of value offerings*, thus it was chosen to create another group of independent variables. One of the variables included in the category is *transparency* on how collected data will be processed and for what reason it is collected. Another one is *value of information disclosure,* which is defined as the individual's overall assessment of the utility of information disclosure based on perceptions of privacy risks incurred and benefits received, or in other words perceived privacy trade-off (Xu et al., 2011). *General privacy concerns* is an important variable in the current environment where users' privacy concerns are increasing and where more attention is drawn to privacy-related issues and companies' misconduct related to user data management. In this case, privacy concerns include attitudes to internet privacy, sensitivity about the way companies handle personal information, and concerns about threats to personal privacy. Lastly, the *privacy fatigue variable* measures emotional exhaustion when dealing with privacy issues.

Table 2
Variables

Dependent variable	Independent variables (content of value offerings)	Independent variables (user perceptions)
• Intent to disclose personal information	• Personalization • Non-personalization (generic) • Hedonic value offering • Utilitarian value offering	• Transparency • Value of information disclosure • General privacy concerns • Privacy fatigue

4.2 Hypotheses

Seven hypotheses were formulated based on the information gathered in the literature review. H1 and H2 treat *personalization* and *hedonic value offering variables* as the primary variables while *non-personalization* and *utilitarian variables* are treated as baseline dummy variables respectively. *Personalization* was chosen as a value that should have a stronger

effect on the *intention to disclose personal information* than *generic, non-personalized value offering,* which we deem to deliver less value to the user. Similarly, based on the findings in the literature, we assume that a *hedonic value offering* that brings enjoyment will have a greater effect on disclosing personal information than *utilitarian value offerings*. It is important to note that there were indications in the researched literature suggesting that the effect of personalization can be both positive and negative, thus we derived two conflicting hypotheses for the personalization variable - $H1_a$ and $H1_b$. Hypotheses ranging from H3 to H6 account for the second group of independent variables measuring user perceptions.

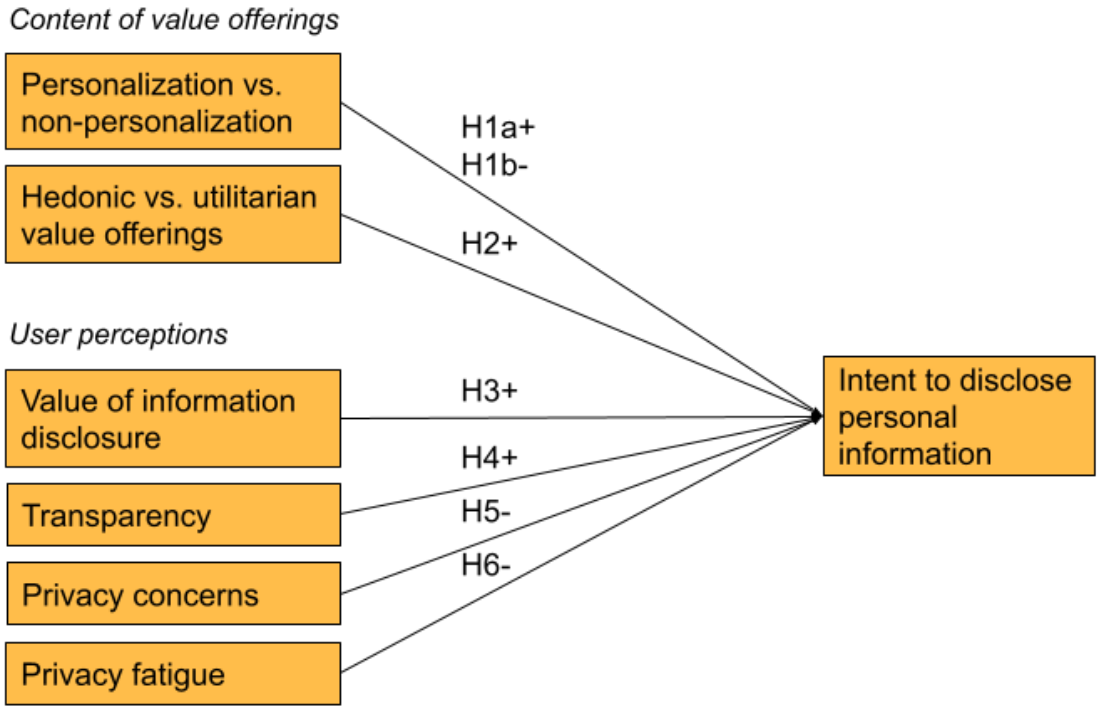
Hypotheses:

- $H1_a$ + : *Personalization* is more positively related to *users' intent to disclose personal information* than *non-personalization*
- $H1_b$ - : *Personalization* is more negatively related to *users' intent to disclose personal information* than *non-personalization*
- H2 + : *Hedonic value offering* is more positively related to *users' intent to disclose personal information* than *utilitarian value offering*
- H3 + : *Value of information disclosure* is positively related to *users' intent to disclose personal information*
- H4 + : *Transparency* is positively related to *users' intent to disclose personal information*
- H5 - : *General privacy concerns* are negatively related to *users' intent to disclose personal information*
- H6 - : *Privacy fatigue* is negatively related to *users' intent to disclose personal information*

Figure 1 represents the research's conceptual framework visually. As mentioned before, independent variables are divided into two main groups, while each independent variable has a hypothetical positive or negative relationship with the dependent variable.

Figure 1

Conceptual framework of the research



5.

METHODOLOGY

RESEARCH DESIGN,
RESEARCH INSTRUMENT FOR THE EXPERIMENT,
RELIABILITY & VALIDITY

5. Methodology

This chapter presents the methodological approaches behind this research of understanding how companies can prepare for a more privacy-focused future and become digital marketing frontrunners. This study follows a mixed-method approach with experimental elements as the quantitative part where hypotheses are tested, and expert interviews of high profiles within the marketing industry as the qualitative part to elaborate on the findings and gain a deeper understanding of the changes within the industry. Furthermore, this chapter presents different layers of the underlying methodology, research design, data collection, data analysis, reliability, and validity related to this study.

5.1 Research design

The research design behind this thesis consists of a mix of quantitative and qualitative research approaches. This is explained further throughout the following sections.

5.1.1 Mixed methods

The research approach for this thesis includes a mix of quantitative and qualitative research methods, known as ‘mixed methods’. Quantitative and qualitative research both have their own strengths and weaknesses. Combining those two research methods can provide a better understanding of the research problem rather than relying on only one of the methods (Bui, 2014). Mixed methods can be a way of generating more complex findings compared to research done by only one method. This happens through triangulation of data, where two different methods are combined to research a phenomenon (Frederiksen, as cited in Brinkmann & Tanggard, 2015). The findings are considered more valid when multiple methods can approve them (ibid.). During this research, the quantitative and qualitative approach will stand individually by default but will have elements of the methods merging when the experts are asked to comment on the findings from the quantitative approach.

5.1.2 Quantitative research approach

The quantitative part of this research entails an online experiment with banners including questions for the respondents to answer in a survey format. A dependent and various independent variables were tested to research any potential effects between them and understand any further correlation. The hypotheses were formulated based on findings from the literature review prior to executing the experiment. These hypotheses were later accepted or rejected according to the analysis results.

The experiment was built as a traditional survey on the platform, Typeform, with elements of randomized exposure to a fictional banner. The survey was collecting results for almost two weeks from March 24 to April 6, 2021 - see appendix A for visuals of the survey. The respondents were first presented with a banner to which only a fourth of the respondents would be exposed to. In total, four banners with different messaging were tested to understand what would trigger users to sign-up for a newsletter. The four different messages were based upon the literature review and analysis of various companies' current value offerings, where four major types of value propositions were highlighted: personalization, generic, hedonic, and utilitarian. Hereafter, the respondents were asked general questions regarding their thoughts on data privacy and online habits. The survey received a total of 149 respondents who were randomly divided into four participant groups to test each banner's value proposition. This random banner assignment to participants eliminates a potential bias and ensures more accurate testing compared to respondents being exposed to all of the banners at once. If the respondents were presented with all four banners, it would be likely that they would start comparing the banners which would not be optimal for objective testing. The respondents were acquired online by sharing the survey on business communication platforms, LinkedIn, Facebook, and Instagram. Thus, the sampling has been a voluntary response sampling based on ease of access which may result in issues in terms of bias, which is explained in section 5.3: Reliability & Validity (McCombes, 2021). The data were statistically analyzed and managed through IBM's Statistical Package for Social Studies (SPSS) software, IBM Statistics 26. Further details of this experiment are explained further in section 5.2: Research instrument for the experiment.

5.1.3 Qualitative research approach

For the qualitative part of this research, we conducted three expert interviews. The informants were chosen to represent three different points of view in this digital marketing and privacy debate. The first informant represented a digital marketing agency, the second represented a business marketing products to consumers, and the third one represented an advertisement platform - in this case, Google. The informants were chosen from a non-probability sampling process, which is a non-random selection of participants (McCombes, 2021). This type of sampling is often used in exploratory and qualitative research where the aim is not to test hypotheses, but instead to develop a deeper understanding of a research topic (ibid.). The individuals were specifically chosen due to their many years of experience in high-profile jobs within the digital marketing industry. This allowed for a deep dive into the research subject with findings based on actual experiences of the experts.

An interview guide was formulated in preparation for the interviews and was adjusted according to each interviewee. The interview guide can be found in appendix B. The interviews were divided into two parts - the first part was a discussion of industry trends, while the second part was a reflection on the findings from the survey. Half of the asked questions were the same for every informant, although some questions were tailored more to the individual interviewee. We chose to repeat the majority of the questions at every interview in order to be able to compare them in the discussion. As an example of tailored questions, the business representative was not asked all the same questions as the Google representative. All three representatives have very different incentives and the privacy-centered future impacts their industries very differently. To connect the qualitative method with the quantitative experiment, the results from the quantitative part of the research were addressed during the interviews allowing the experts to explain their take on the findings.

The duration of the interviews was approximately 30 minutes each and they were all hosted virtually on either Google Meet or Microsoft Teams. The interviews were conducted in a semi-structured manner whereas we as researchers had formed an interview guide that was primarily used to lead the interview. We would then ask the interviewee to elaborate on areas we found important for this research. According to Saunder et al. (2016), research interviews

can be an effective way of gathering valid and reliable data relevant to a research question. Furthermore, the interviews can be helpful when expanding and refining ideas for the research. The narrative data gathered from the interviews were transcribed and categorized into different themes to compare the opinions to each expert and discover where there was a common alignment, disagreement, or an original point of view expressed. The results of the major themes of the interviews can be found in section 6.2: Interview findings. Quotations were selected from the interviews that highlighted the concepts relevant to answering the research question.

5.2 Research instrument for the experiment

The research questionnaire was constructed based on the questions found in the reviewed literature. The *content of value offerings* independent variables' effect on the dependent variable was measured by randomly showing survey participants one out of the four banners with a specific value proposition (either personalization, generic, hedonic, or utilitarian) and then asking them to answer questions related to *intention to disclose personal information* in the scenario.

Followingly, the second group of independent variables on *user perceptions* such as *value of information disclosure*, *transparency*, *general privacy concerns*, and *privacy fatigue* are measured. Lastly, additional questions such as frequency of visiting online stores, previous privacy experience, age, gender, and country of residency were asked to get an overview of the demographics of the sample.

Each question was measured on a 7-point Likert scale ranging from “completely disagree” to “completely agree”. This scale was chosen since it was the most commonly used by the authors that are referenced and because it provides enough variance which is useful when analyzing the data.

Table 3
Research questionnaire

Questions	Variables	Authors
1. I am willing to disclose personal information asked by the online retailer to receive the newsletter. 2. I will likely disclose personal information asked by the online retailer to receive the newsletter.	Intention to disclose personal information	Choi et al. (2018)
1. I think my benefits gained from the use of the mentioned online shop can offset the risks of my information disclosure. 2. The value I gain from the mentioned online shop is worth the information I give away.	Value of information disclosure	Xu et al. (2011)
1. It is important to me whether a site tells me how long they will retain information they collect from me. 2. It is important to me what is the purpose for which the site wants to collect info from me.	Transparency	Awad & Krishnan (2006)
1. All things considered, the Internet causes serious privacy problems 2. Compared to others, I am more sensitive about the way online companies handle my personal information 3. I believe other people are too concerned with online privacy issues (reverse coded) 4. I am concerned about threats to my personal privacy today	General privacy concerns	Sanchez et al. (2019)
1. I feel emotionally drained from dealing with privacy issues in an online environment 2. It is tiresome for me to care about online privacy	Privacy fatigue (exhaustion)	Choi et al. (2018)
Additional questions:	**Variables**	**Authors**
How often have you personally been victim of what you felt was an invasion of online privacy?	Previous privacy experience	Xu et al. (2011)
How much have you heard or read during the last year about the use and potential misuse of personal information about consumers?	Previous privacy experience	Xu et al. (2011)

The respondents were exposed to banners in the context of newsletter subscription for a fictional online shop. Newsletter signups are one of the main ways companies collect user information in an opt-in way for their customer relationship management (CRM) databases. This data can later be used not only to communicate with users via newsletters but also for targeting through digital ads. Another reason for choosing newsletter signups was due to the decision to experiment with upper-funnel marketing practices where users could potentially

provide personal data without a higher level of involvement with the business such as creating a profile. Additionally, the personal data required to sign up for a newsletter could be minimized to only providing an email, which not only makes the process fast but most importantly minimizes the risk of users being reluctant to provide certain types of data that they would not be comfortable with. Alternatively, it was considered to create the experiment using banners for cookie tracking opt-in but after reviewing numerous banners in some of the most popular online shops listed in table 4, it was decided that there is little creative variety in the messaging. Moreover, what has to be declared in the banners is strictly defined in the Electronic Privacy Directive and, from our own observations and experience, users are used to quickly accepting or declining the cookie banner terms instead of analyzing the content of the terms and conditions.

Before designing the banners, we reviewed and classified what newsletter sign-up value propositions are used by the most popular e-commerce websites in Denmark, Sweden, and the United Kingdom (E-commerce News, 2019). Only relevant banners were included in the review, while some additional smaller e-commerce websites were added for variety and inspiration.

Table 4

Value propositions in newsletter sign-up banners

Company	Context	Value proposition	Classification
Bang & Olufsen	Luxury consumer electronics	Product news, updates, special invites	Generic
CDON	Fashion, beauty, home, electronics, sports, and more	Promotional news, offers, tips, news, priority for promotions	Generic
John Lewis	Fashion, beauty, home, electronics	Inspiration, new arrivals, offers	Generic
Mango	Fashion	Exclusive promotions, news, access to sales	Generic
Webhallen	Consumer electronics	No value proposition	Generic
Nemlig	Food	No value proposition	Generic
MyTheresa	Luxury fashion	Get trend updates and style tips	Generic, hedonic

Otto	Fashion, home, electronics	Secure benefits	Generic
Saxo	Books	Book love to your inbox	Generic
Goodie Box	Beauty products subscription	Get love to your inbox	Generic
Marks & Spencer	Fashion, food, home	Offers tailored to you, rewards, promotions before anyone else	Generic, personalization
Marks & Spencer	Fashion, food, home	10% discount	Utilitarian
Boozt	Fashion, beauty	10% discount	Utilitarian
H&M	Fashion, beauty, home	25% discount and free delivery	Utilitarian
Zalando	Fashion, beauty	10% discount	Utilitarian
Nakd	Fashion, beauty	20% discount, news, offers	Utilitarian, generic
Farfetch	Luxury fashion	Access to sales and new arrivals first	Personalization
Komplett	Consumer electronics	Personalized news, offers and discounts, lottery draw	Personalization, hedonic

As a result, it was decided that personalization would be best represented by indicating value propositions that are defined more precisely than the generic ones and that include the keyword “personalized” in the text. In contrast, the generic banner included messaging that was the most common among online retailers who have taken such an approach - offering news and offers without specifying anything particular. The utilitarian banner was decided to include a 10% discount as it was often done by e-commerce retailers. It was a bit more challenging to define a hedonic value proposition since there were not many sites offering such. It was decided to be a free branded tote bag, which does not bring direct monetary gain as the utilitarian value proposition but rather adds value in a form of a gift that might provide enjoyment. Lastly, it was chosen to present survey participants with an imaginative scenario when they are exposed to the banner and asked to indicate their willingness to provide their personal information. The context for the imaginative scenario was chosen to be a new fashion online shop that has caught the user’s interest. Our experimental banner only asked users to provide email since that is the minimum required information to target users through newsletters and digital ads. The experimental banners can be seen below in figure 2.

Figure 2

Banners for content of value offerings

5.3 Reliability and validity

The survey sampling was a voluntary response sampling which can lead to biased results. As an example, the survey was shared on social media and business communication platforms which made some people voluntarily participate for various reasons. When sharing surveys on social media, one might risk that the respondents are expressing very similar opinions due to *filter bubbles*, since social media platforms are programmed to push content to similar users who engage with a post (Pariser, 2011). Furthermore, a group of the respondents could be some who have very strong opinions around the topic of data privacy and therefore do not represent the general public's opinions. Another biased factor is the possibility that close friends and family may impact the result to accommodate what they believe we as researchers would like them to answer. We tried to avoid this by not mentioning anything of importance related to the results when distributing the survey. With the respondents' limited knowledge of the aims of the research, they have hopefully been as honest as possible when

answering. Avoiding a bias completely is a big challenge to any research and cannot always be possible to achieve.

Conducting semi-structured interviews may lead to concerns regarding the reliability of the data collected. It can be questioned whether other researchers would achieve similar results and whether the findings were biased. When informants are chosen non-randomly, the risk of sampling bias increases. This makes it more difficult for other researchers to replicate the research, while the conclusions can be more limited and do not directly represent a general opinion. Our attempt to limit sampling bias was to investigate different sides of the industry, hence participants from an agency side, business side, and advertisement platform side. They may be experiencing different challenges and have contradicting views on this privacy-focused era. When analyzing the data from the interviews, personal bias is a validity threat that can be hard to overcome. This is due to the subjectivity of our own experiences, assumptions, and beliefs that can influence how we as researchers analyze, interpret and present the results (Bui, 2016). A semi-structured interview will often have obstacles related to bias since the interviewer leads the discussion using the questions of their choice and by asking follow-up questions that may hint to the informant of the presumptions from the interviewer’s side.

6.

ANALYSIS

SURVEY & INTERVIEW FINDINGS

6. Analysis

This chapter covers a description of how both the quantitative and qualitative data were analyzed. Furthermore, this chapter presents the concluded findings.

6.1 Survey

An online survey was utilized for the quantitative part of this research. The survey was structured into two main parts - an experiment, where each respondent was shown one of the four banners with different *content of value offerings*, and a part where various privacy-related *user perceptions* were examined. The results from both parts of the survey were later analyzed to discover what makes users *willing to disclose their personal information* (e-mails in this experiment). It is important to note that the survey results were analyzed using IBM's Statistical Package for Social Studies (SPSS) software in order to go beyond only descriptive statistical analysis and to utilize inferential statistics in order to explore relationships between variables. More details regarding the distribution and execution of the survey can be found in section 5.1.2: Quantitative research approach. In the following sections, it is explained how the hypotheses were tested followed by a presentation of the results.

6.1.1 Respondent characteristics

The respondents were recruited through a voluntary response sampling technique, where they willingly accepted the request to join the sample. The survey has been completed by 149 respondents. 70% (105) of them currently reside in Denmark, 15% (22) respondents reside in Lithuania, 5% (7) in the United Kingdom while the rest live in Belgium, Estonia, Germany, Italy, Norway, Portugal, Finland, Sweden, United States, and Spain.

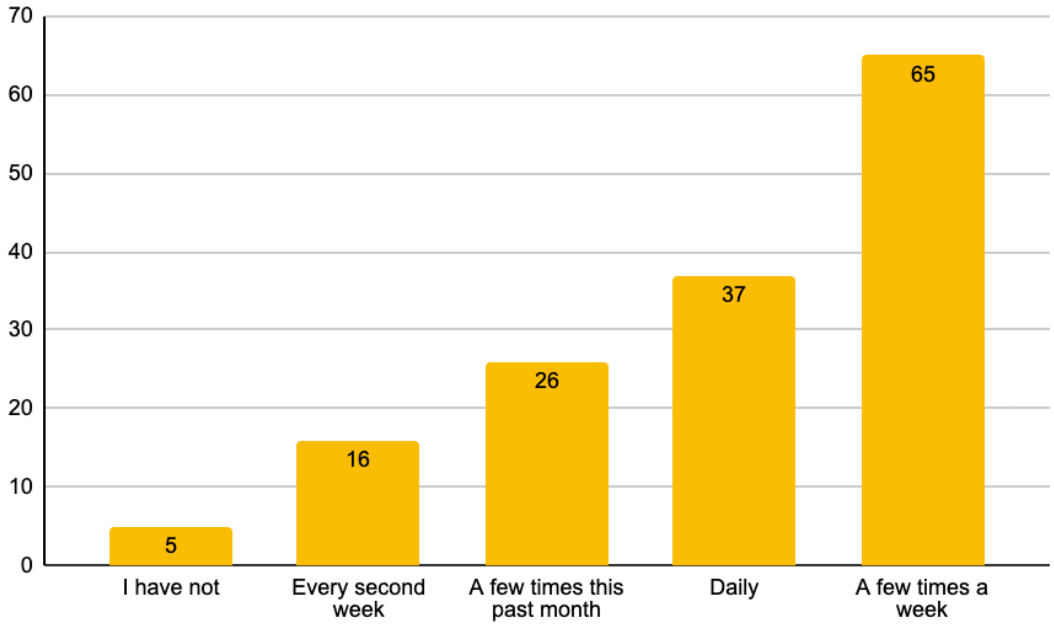
The average age of the respondents was 29 years, while the median was 25 years. The youngest respondent was 18 years old, while the oldest was 74 years. 63% (94) of the respondents identified themselves as female, 36% identified as male (53), while 1% (2) identified as other.

6.1.1.1 Online shopping habits

The respondents were asked to estimate how often they have visited online stores in the past month including any kind of e-tailers providing both products and services. The results are represented in figure 3 below, where it is visualized that most of the respondents are rather frequent visitors of e-commerce web pages. The majority of the respondents say they visit online shops a few times a week.

Figure 3

Frequency of e-shop visits



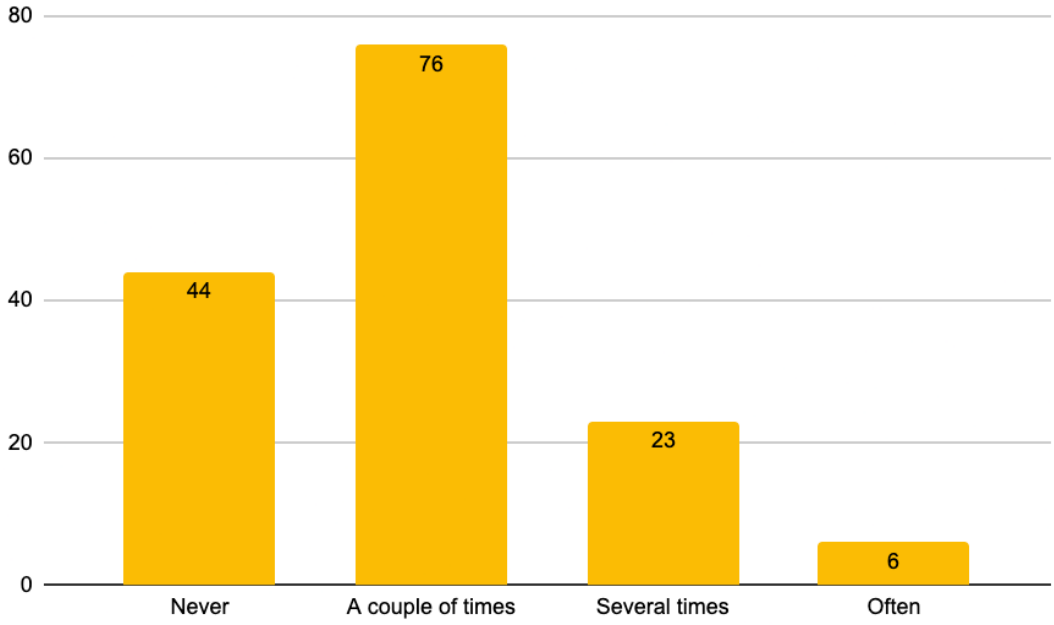
Question: How often have you visited online shops in the past month? Examples of online shops: online retail stores, food delivery services, booking a service, etc.

6.1.1.2 Invasion of privacy

Another aspect of respondent characteristics was their previous privacy experiences. 70% (105) of the respondents felt that their online privacy has been invaded at least a couple of times previously. However, the data is centered around people who have not experienced privacy invasion very often - only 19% (29) felt that invasion of their privacy was highly repetitive. In contrast, 30% (44) never have felt that their online privacy was invaded.

Figure 4

Respondents' perceptions on being victims of invasion of privacy



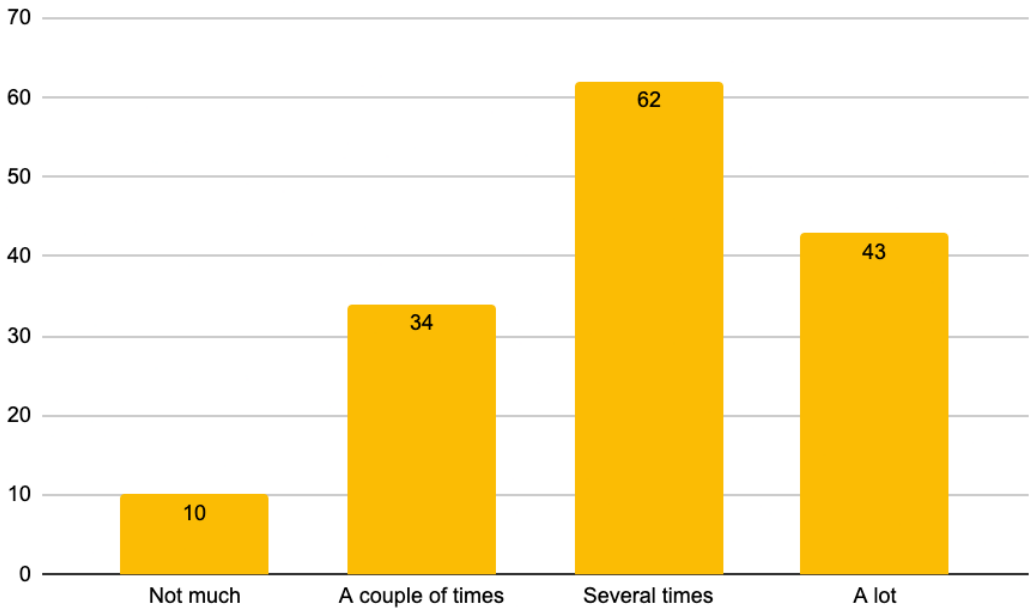
Question: How often have you personally been a victim of what you felt was an invasion of online privacy?

6.1.1.3 Privacy issues related to the internet

The survey data shows that respondents are highly aware of privacy issues in the online environment and potential misuses of user personal information. Only 7% (10) of the respondents have not heard about any online privacy violation in the past year, while 70% (105) have been informed about it repetitively.

Figure 5

Respondents' awareness about the potential misuse of personal information



Question: How much have you heard or read during the last year about the use and potential misuse of personal information about consumers?

6.1.2 Measures of central tendency and reliability

Each variable, besides the independent ones that were measured by showing one out of four banners randomly, was measured by asking two to four questions. The answers were ranked on a 7-point Likert scale ranging from 1 - "completely disagree" to 7 - "completely agree". In this section, the internal consistency of the scales and descriptive statistics provided by the answers are analyzed.

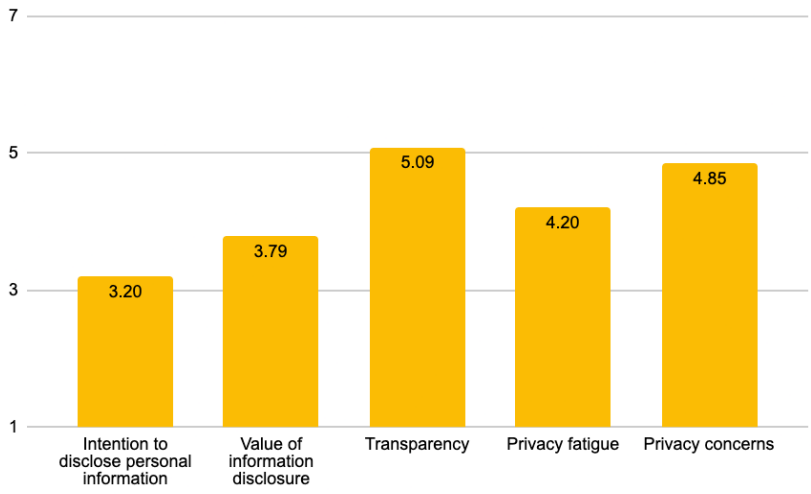
A summary of the internal consistency of the items measuring variables is presented in table 5. Reliability coefficient Cronbach's Alpha is considered acceptable if it is 0.7 or above. In general, all scales except privacy fatigue are reliable.

Table 5
Reliability statistics

Variable	Cronbach's Alpha	Cronbach's Alpha based on standardized items	N of items
Intention to disclose personal information	.905	.905	2
Value of information disclosure	.752	.754	2
Transparency	.737	.743	2
General privacy concerns	.746	.744	4
Privacy fatigue	.623	.627	2

Some insights can be drawn by looking at the variables as standalones. In figure 6 below, it can be observed that the *transparency* variable has the highest average value indicating that respondents most commonly agreed with its importance. The *privacy concerns variable* also has a relatively high mean indicating that the statements provided in the questionnaire were supported by the respondents. *Privacy fatigue* and *value of information disclosure* averages are centered around the middle of the scale thus little insights can be gained by only looking at the means. *Intention to disclose personal information* is the dependent variable that was influenced by the banners shown to the respondents in a randomized way thus independent variables have to be taken into account when making any conclusions.

Figure 6
Means of variables



6.1.2.1 Intention to disclose personal information

The dependent variable named *intention to disclose personal information* was measured after showing a randomized banner offering a regular newsletter subscription. It was measured by two questions that are proven to be internally consistent and thus highly reliable with a Chronbach's Alpha of 0.905.

Table 6
Item statistics for the dependent variable

Item	Mean	Median	Standard Deviation	N
Intention to disclose personal information I	3.23	3	2.119	149
Intention to disclose personal information II	3.17	2	2.061	149

A relatively high standard deviation is influenced by the independent variables - as mentioned before, each respondent got a randomized banner. The personalization banner was shown to 37 respondents, generic to 37, hedonic to 41, and utilitarian to 34. Before running linear regressions it is already visible that respondents had a rather negative tendency to share their private information, especially when they received personalization banners. The utilitarian banner featuring a 10% discount seems to have received the highest intention to disclose personal information scores by looking at the highest mean and median among the items.

It is important to note that table 7 represents results for the variables as standalones. In section 6.1.4: Multiple linear regression analysis, it is explained how these variables relate to the dependent variable when analyzing the level of significance.

Table 7

Statistics based on content of value offerings independent variables

Dependent variable items	Personalization	Generic	Hedonic	Utilitarian
Intention to disclose personal information I				
Mean	2.68	3.30	3.17	3.85
Median	2	3	2	4
Standard deviation	2.028	2.129	2.174	1.927
Intention to disclose personal information II				
Mean	2.57	3.03	3.41	3.68
Median	2	2	3	4
Standard deviation	1.882	1.952	2.197	1.981

6.1.2.2 Value of information disclosure

The *value of the information disclosure* scale is reliable, however not much can be determined from descriptive statistics since the answers are centered around the middle of the Likert scale which indicates a "not sure" answer from the respondents. Item statistics, including information such as mean, median, and standard deviation, for the independent variables can be found in table 8.

6.1.2.3 Transparency

Transparency is another scale with sufficient reliability. Moreover, items of the scale provide additional information about the respondents. Users find it rather important to be informed how long a site will retain information that is collected from them (measured by the first item) - 57% chose answers agreeing with the statement above 4 on the Likert scale (representing answer "not sure"). Additionally, users find it even more important to be informed about the purpose for which the site wants to collect information from them - 82% of the respondents chose answers agreeing with the statement (the second item).

6.1.2.4 General privacy concerns

The *general privacy concerns* scale achieved sufficient reliability after the third item was coded in reverse. Some insights can be drawn from descriptive analytics regarding this variable. Clearly, respondents were concerned about the seriousness of the problems that the internet causes - 86% chose answers agreeing with the statement (measured by the first item). It varied whether respondents saw themselves as more concerned about the way online companies handle their personal information in comparison with others since the answers were distributed rather equally (second item). 61% of the respondents disagreed that to their belief others are too concerned about privacy (third item). Lastly, respondents were concerned about their own personal privacy (fourth item) since 64% of them chose a measurement above 4 on the Likert scale while only 32% chose measurement below 4.

6.1.2.5 Privacy fatigue

Privacy fatigue was the only variable that did not receive a sufficient Cronbach's Alpha, therefore it was decided to use only the second item measuring privacy fatigue in the further research. The second item was chosen due to higher mean and median and lower standard deviation. Also, critically reflecting on the questionnaire, the first item was measured by asking respondents whether they feel "emotionally drained" from dealing with privacy issues in the online environment, which might have been a relatively strong statement in comparison with the second item measuring if respondents are simply "tired" from dealing with privacy issues.

Some insights can be drawn from the items separately. Even though the respondents' answers to the question asking if they feel emotionally drained from dealing with privacy issues in an online environment were distributed quite equally on the Likert scale, it can be observed that 47% chose answers disagreeing with the statement, while in contrast, 38% chose answers agreeing with the statement. When asked if it is tiresome for them to care about online privacy, 58% agreed that it is, while only 28% chose answers on the negative side of the scale.

Table 8
Item statistics for user perceptions independent variables

Item	Mean	Median	Standard Deviation	N
Value of information disclosure I	4.01	4	1.736	149
Value of information disclosure II	3.56	4	1.904	149
Transparency I	4.58	5	1.963	149
Transparency II	5.59	6	1.681	149
Privacy concerns I	5.77	6	1.317	149
Privacy concerns II	4.13	4	1.898	149
Privacy concerns III	4.80	5	1.746	149
Privacy concerns IV	4.71	5	1.789	149
Privacy fatigue I	3.90	4	1.989	149
Privacy fatigue II	4.50	5	1.746	149

6.1.3 Correlation between variables

A correlation between variables or, in other words, the strength of a linear association between two variables was measured by Pearson correlation. It is commonly defined that a correlation between 0.1 and 0.3 is small, while a correlation between 0.3 and 0.5 is medium and above 0.5 is strong. Detailed results of the Pearson correlation can be found in appendix C.

In this case, only *personalization* and *value of information disclosure* have a significant correlation with the dependent variable *intention to disclose personal information*. *Personalization* has a negative small correlation, while *the value of information disclosure* has a strong positive correlation with the dependent variable. It can be seen that some of the independent variables also have significant correlations - *personalization* and *hedonic*, *privacy concerns* and *transparency, privacy concerns* and *privacy fatigue, privacy concerns,*

and *value of information disclosure*. In order to prevent multicollinearity, VIF and Tolerance values are determined when running the regressions.

6.1.4 Multiple linear regression analysis

Multiple linear regression analyses were conducted in order to test the hypotheses. As mentioned before and pictured in the research conceptual framework (figure 1), independent variables were divided into two groups of *content of value offerings* and *user perceptions*, thus multiple linear regressions were run for each group of the variables accordingly.

6.1.4.1 Content of value offerings

A multiple linear regression analysis was conducted in order to test the effect that the content-related independent variables might have on the dependent variable. The independent variables were coded as dummies, where *personalization* received a value of 1, while the corresponding baseline *non-personalization* (or generic) variable received a value of 0. The same was applied to the *hedonic variable* that was coded as 1, while the *utilitarian variable* received a value of 0.

Looking at the model's fit to data, it is visible that R, which is a measure of strength and direction of the linear relationship between two variables, is positive but relatively weak (a strong one would be considered above 0.7). Adjusted R square indicates what percentage of the dependent variable can be explained by the independent variables. In this case, it is 2,9% which is a relatively small value, indicating that the predictors might not have a substantial effect on the dependent variable. Lastly, Durbin Watson, a measure of autocorrelation, is close to 2, which signals that the model is independent of errors.

Table 9
Model's fit to data

Predictors	R	R square	Adjusted R square	Durbin Watson
Personalization, Hedonic	.171	.029	.016	1.852

An ANOVA analysis of variance shows that the linear regressions did not achieve a required significance level (95%) thus meaning that it cannot be used to explain a significant amount of variance.

Table 10
ANOVA

Model	df	Mean square	F	Sig.
Regression	2	8.596	2.189	.116
Residual	146	3.926		
Total	148			

It is visible in table 11 that the *personalization* variable has achieved a required significance level of at least 95%. In contrast to some of the predictions, both *personalization* and *hedonic* value offering have a negative effect on the *intent to disclose personal information*. *Personalization* has achieved the required significance level at 95,9% thus it can be stated that *personalization*, compared to *generic value offering*, has a negative effect of -0.829 on *intention to disclose personal information*. In addition, collinearity statistics indicate that there are no multicollinearity issues since tolerance is above 0.2 and VIF is below 2 and just slightly above 1.

Table 11
Coefficients

Independent variable	Unstandardized coefficients		Standardized coefficients	t	Sig.	Collinearity statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	3.451	.235		14.674	.000		
Personalization	-.829	.402	-.180	-2.064	.041	.875	1.143
Hedonic	-.158	.389	-.035	-.407	.685	.875	1.143

Based on the analysis above, hypotheses H1a+ and H2 are refuted. *Personalization* and *hedonic value offerings* are not positively related to the *intent to disclose personal information*, while *hedonic value offering* has no significant effect. Hypothesis H1b- is confirmed since *personalization* has a negative significant effect on *intention to disclose personal information*.

6.1.4.2 User perceptions

Another set of independent variables named *user perceptions* were investigated using multiple linear regressions. In table 12 representing the model's fit to data it is already visible that R square is notably higher than it was for the previous model - dependent variable can be explained by the predictors at 39% in comparison with 2,9% that were generated by the previous model. In addition, the Durbin Watson test indicates that residuals are not correlated, since the value is close to 2.

Table 12
Model's fit to data

Predictors	R	R square	Adjusted R square	Durbin Watson
Value of information disclosure, Transparency, Privacy concerns, Privacy fatigue	.624	.390	.373	1.864

ANOVA variance analysis for the new model is significant, proving that it can be used to explain a significant amount of variance.

Table 13
ANOVA

Model	df	Mean square	F	Sig.
Regression	4	57.527	22.988	.000
Residual	144	2.502		
Total	148			

The *value of the information disclosure* variable achieved the highest level of significance thus it can be stated that it has a positive relationship with the dependent variable. According to the results, a change of one standard deviation in *value of information disclosure* will result in a change of 0.774 standard deviations in *intention to provide personal information*. *Privacy fatigue* has also achieved the required level of significance, thus for every one-unit increase, the dependent variable will decrease by -.160. *Transparency* and *privacy concerns* do not have a significant relationship with the dependent variable. In addition, collinearity statistics indicate that there are no multicollinearity issues since tolerance is above 0.2 and VIF is below 2 and just slightly above 1.

Table 14
Coefficients

Independent variable	Unstandardized coefficients		Standardized coefficients	t	Sig.	Collinearity statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	1.080	.724		1.429	.138		
Value of information disclosure	.774	.083	.632	9.372	.000	.933	1.072
Transparency	.041	.091	.034	.452	.652	.768	1.303
Privacy concerns	-.062	.117	-.040	-.530	.597	.754	1.327
Privacy fatigue	-.160	.076	-.140	-2.104	.037	.961	1.040

6.1.5 Moderation and mediation analyses

In addition to researching the direct effect that independent variables have on *intention to disclose personal information* as planned in the conceptual research framework, it was decided to pursue mediation and moderation analyses. The aim of these analyses is to find out whether variables measuring *user perceptions*, specifically *value of information disclosure*, *transparency*, *general privacy concerns,* and *privacy fatigue*, could potentially moderate and/or mediate the relationship between *content of value offerings* category of independent variables and the dependent variable.

6.1.5.1 Moderation and mediation effects for personalization

The moderating effect occurs when a third variable changes the direction or magnitude of the relationship between two variables (Zainudin, 2016). To analyze moderation effects, variables were standardized and interaction between *personalization* and moderation variables was calculated by multiplying each pair of the values. Then four multiple regression models

including *personalization*, one of the moderation variables, and the interaction variable were run. Tables showing detailed results can be found in appendix D. However, no significant moderation effects were found.

Mediation is a hypothesized causal chain in which one variable affects a second variable that, in turn, affects a third variable (Newsom, 2020). The intervening variable is called mediator (Newsom, 2020), which mediates the relationship between a predictor and outcome variables. To analyze mediation effects PROCESS version 3.5.3 written by Andrew F. Hayes (2018) was installed. A matrix procedure was executed, where direct and indirect effects of the independent variable on the dependent variable were calculated. As a result, none of the four potential moderation variables proved to have a significant effect (appendix E).

6.1.5.2 Moderation and mediation effects for a hedonic value offering

To analyze the moderation and mediation effect for *hedonic value offering*, the same procedures were carried out as it was done with the *personalization* variable. As a result, none of the four variables showed significant moderation or mediation effects. Tables showing detailed results can be found in appendix F and G.

6.1.6 Conclusion of the quantitative analysis

Three out of seven hypotheses were accepted with sufficiently significant results, while the others were rejected. The results of the hypothesis testings are represented in table 15. It was found that the *value of information disclosure* is positively related to users' *intent to disclose personal information*, while *personalization* and *privacy fatigue* are negatively related. Moreover, mediation and moderation analyses proved that *user perceptions* group of variables are indeed independent variables having a direct effect on the *intention to disclose personal information*.

Table 15
Summary of hypothesis testing

$H1_a$ +	*Personalization* is more positively related to users' *intent to disclose personal information* than *non-personalization*	Rejected
$H1_b$ -	*Personalization* is more negatively related to users' *intent to disclose personal information* than *non-personalization*	Accepted
H2 +	*Hedonic value offering* is more positively related to users' *intent to disclose personal information* than *utilitarian value offering*	Rejected
H3 +	*Value of information disclosure* is positively related to users' *intent to disclose personal information*	Accepted
H4 +	*Transparency* is positively related to users' *intent to disclose personal information*	Rejected
H5 -	*General privacy concerns* are negatively related to users' *intent to disclose personal information*	Rejected
H6 -	*Privacy fatigue* is negatively related to users' *intent to disclose personal information*	Accepted

6.2 Interview findings

To obtain a deeper understanding of the findings from the quantitative part of this research, expert interviews are utilized to discuss the results as explained in section 5: Methodology. Furthermore, the expert interviews were benefiting this research by expanding on privacy-related industry topics and sharing their own experience from their many years of working in the field of digital marketing. This allowed for a deep dive into this research area while refining recommendations for future-proofing businesses as presented in section 7: Discussion. When analyzing qualitative data in a narrative form, reporting findings is advised to be done by organizing the data into major themes and patterns (Bui, 2016). The themes are not decided prior to analyzing but will emerge during the data analysis process. It is advised to focus on 5 to 6 major themes when applicable to the research question. After the major themes have been presented, a *thick description* will follow. The thick description includes an explanation of the context and a quote from the informant to underline the presented

argument (ibid.). The quotes are derived from the transcriptions of the three interviews which can be found in appendix H, I, and J.

6.2.1 Presenting the experts

The experts chosen for the interviews represented different sides of the digital marketing industry - a digital marketing agency that performs marketing consultancy work for clients, a business heavily investing in and relying on digital marketing, and a large advertising platform. The following sections present each of the three experts and explain their background including why they are relevant for this research.

6.2.1.1 Rhys Cater, Managing Director of Precis Digital London

The first interview was conducted with Rhys Cater, who is a managing director and partner of a digital marketing agency named Precis Digital. Precis Digital was founded in Stockholm in 2012 and has since grown to have more than 300 employees across 8 offices in Europe. The digital marketing agency has been internationally acknowledged by various digital marketing award organizations. To name a few, they have won the Drum's Media Agency of the Year 2020 and Best Large PPC Agency in Europa by the European Search Award in 2017, 2018, and 2019.

Rhys Cater has been in charge of the London office for approximately four years. Prior to this position at Precis Digital, he worked at Google as a Solution Consultant for six years. His primary expertise lies within digital marketing, data analytics, and digital strategy. His educational background is a Bachelor of Arts within Modern and Medieval Languages at The University of Cambridge.

6.2.1.2 Morten Køhler Hansen, Display Marketing Manager at Bang & Olufsen

Morten Hansen has been the Display Marketing Manager at Bang & Olufsen for 2,5 years. Bang & Olufsen is a Danish company that designs, manufactures, and sells high-end electronic devices such as headphones, speakers, and televisions. The company was founded in 1925 and has since then been popular around the world for its luxurious design. Bang & Olufsen has a strong brand reputation but has been struggling financially the last decade due

to rising competition. The company has started focusing on various e-commerce and digital activities in the past few years, while steadily growing its digital department. Digital marketing has recently become an important component for Bang & Olufsen for all marketing funnel activities - from increasing brand awareness to driving conversions. In the past financial year, the company has reported double-digit percent revenue growth every quarter (Bang & Olufsen A/S, 2021). We included Morten Hansen in our expert panel as a representative of a business side of the digital marketing and privacy debate.

Morten Hansen's educational background is Master's of Brand and Communication Management from Copenhagen Business School and he has extensive experience in project management, media buying, and optimization. Currently, Hansen is responsible for display marketing activations on various social media platforms (Facebook, Instagram, Pinterest, LinkedIn, Youtube, TikTok, etc.), while being the main force when adapting various privacy-first practices. Hansen manages many stakeholders such as the legal, IT, data insights departments and agencies to adapt to the ever-changing digital marketing landscape and implement privacy-related practices.

6.2.1.3 Thomas Bering, Nordic Head of Performance & Privacy lead at Google

Thomas Bering's official title is Nordic Head of Performance at Google. Although, he explains his role as the Brand Measurements Full-funnel Lead for the Northern Europe Region and the Privacy Lead for the Danish market. After having worked at Google for more than 16 years with various privacy-concerned clients, he is a very competent informant to discuss this research subject. His role as a Privacy Lead for the Danish market entails communicating with the Danish team how to address privacy-related issues with clients and educating them on the changes happening internally.

Thomas Bering is representing a leading advertising platform during this discussion and shares Google's take on the online privacy debate. His educational background is a Master's of Art in English, Philosophy, and Informatics at Aarhus University.

6.2.2 Theme 1: Current and future challenges for marketers

The very first question we asked the experts after having them introduce themselves was: "What do you believe are the biggest challenges for digital marketers right now?"

To answer this question, Rhys Cater, our first interviewee, explained that digital marketing as a discipline has grown into being way more complex than it used to be. His experience from a digital marketing agency showcased that it has grown into more technical depth thus understanding the current changes in the digital marketing landscape can be a big challenge for the average marketer. Marketers have to formulate a very strong idea of what the business is trying to accomplish with their marketing efforts, build the strategy, coordinate with other departments, align budgets, execute the campaign, and then analyze the performance. Many say that the Chief Marketing Officer (CMO) has one of the absolute most difficult jobs, and Rhys agrees to this statement: *"It's a really, really complex job. You often hear thrown about that CMOs have the hardest job in any company. I don't know if that's just people being biased, but you know, I'm prepared to believe it because their scope is so wide."* (full interview transcript is presented in appendix H)

Rhys Cater adds to this statement that the whole privacy agenda has made the job even more complex. Now marketers have the pressure of being technical experts and on top have to know the latest legislation on user privacy, e.g. cookie consent. One thing is the challenging aspect of learning the legislation, but translating it to what a company does can be even more tricky, Rhys Cater explains: "*Translating what that legislation and what the changes in technology regarding privacy, and what changes in consumer expectations actually mean, for the work that they're doing day to day? That's a huge challenge*." He concludes his answer by saying: "*So I suppose to put it quite simply, the biggest challenge that digital marketers face today, I think, is that they're expected to do far too much stuff. And often they are under-resourced and underprepared."*.

Our second interviewee, Morten Hansen, answers this question by discussing the elimination of cookies: *"It's about adjusting to a cookieless future. That is one of the biggest challenges. All of the big platforms have announced that they want to discontinue it, at least from 2022.*

So that is one of the big things on our radar" (full interview transcript is presented in appendix I). He sees the cookieless future as a threat to personalization. He acknowledges that first-party data will grow in importance but it will be a challenge for them to get the same results without cookies: *"Because that is in some platforms, where we've had to be in anyways, it simply isn't possible to add first-party data or really utilize it in a big scale way. So we have to use more contextual targeting."*. He states that Google can easily ban others from using their third-party cookies but the company still keeps their collected data about users: *"And it's also about talking about platforms. What kind of data do they collect in general? And how much do they offer you to use as a marketer as well? Google has like the vast amount of that, right? They have the search engine, which is a big pool of data. So if you could be honest, you could say it's easy for Google to release cookie data and go cookieless because they pretty much can collect that data anyway through what people are searching."*. To sum up from his answer to this question: cookies going obsolete is a big challenge to the marketers which affects all businesses except the biggest data collectors themselves e.g. Google. Morten Hansen believes that this change of cookie usage is heavily instructed by the enforcement of GDPR: "*I've been working with this now for the last six-seven years and it's interesting to see how it started out with them (Google) focusing more and more on targeting the individual and giving an individual an ID and using that. So the European Union started talking about how they don't really want to see that development and introducing GDPR. Then rolling out GDPR. And now seeing that they closed all of that down.*".

The last interviewee, Thomas Bering from Google, ironically answered the question of marketers' biggest challenges by saying that: "*The easy answer is that the loss of cookies and tracking and everything are the biggest challenges. That I think also feels a bit as a boring answer {...} The biggest challenge is that anyone who's worked with digital marketing for any amount of time for the last 5-10-15, maybe even 20 years, has been used to being able to measure everything, and all discussions and planning has been around, moving closer and closer to the personalized marketing {...} And all of a sudden, that entire foundation has been ripped away from them.*" (full interview transcript is presented in appendix J). He acknowledges that cookies going obsolete is a big change for marketers but he emphasizes that the change of mindset is an even bigger challenge. He states that everyone who has

learned to do marketing “the old way” will have to adapt to new ways of thinking. None of the marketers can change the legislation, therefore it is more productive to accept it and adapt to the way digital marketing is evolving.

To sum up the experts’ opinions on challenges for marketers, every informant admitted that many changes are happening within the field, which can be very difficult to adapt to. Furthermore, they all mentioned that new legislation and the prevention of cookie tracking is on top of every marketer’s agenda as a problem that needs to be tackled.

6.2.3 Theme 2: Solutions to these challenges

Following the discussion around challenges, a solution-oriented question was asked: “We have noticed many privacy-first solutions emerging right now. New tracking-free browsers, differential privacy, FLoC-technology to mention a few. What do you believe could become an industry-standard in the future?“.

There are many emerging technologies that try to mitigate the loss of data that will happen when third-party cookies go completely obsolete, as Rhys Cater sees it: “*I think the honest answer is that we might struggle to converge around an industry standard for some time. If you think about the incentives that Google has, versus the incentives that Apple has, I can't imagine them coming together in the short term, and finding a solution that Apple's happy to implement in Safari, and that Google is happy to implement in Chrome. So I actually think that we might end up quite some time with a bit of a two speed system, where people using different browsers end up with differing levels of data usage and capabilities when it comes to marketing.*”. Google is behind the development of FLoC (explained in section 2.3.2), which Rhys Cater meets with skepticism: “*If you look at what FLoC is trying to do, it's trying to enable that same behavior. But by using a different set of technologies. It's stuff that happens locally in the user’s browser, rather than bouncing data around on servers. I'm quite skeptical about FLoC. I think that FLOC is obviously an interesting, technical solution. And I think if what the purpose of what consumers wanted, and the purpose of lawmakers was to end up exactly as we are today, but without using third-party cookies, then it would be a great solution. But that's not really what these laws are about, right? If you think about what most*

people care about with privacy, it's who has access to their data, and what it is used for. FLoC enables their data to be used for the same purpose as it was before just in a bit of different way.". To sum up Rhys Cater's opinion on FLoC as a solution: he does not think that FLoC is solving the right problem if it is invented to protect and serve the user's best interest.

The second informant, Morten Hansen, also shared the same opinion that these new solutions are not always as beneficial to the user as they have been praised to be: *"So you could also argue, are we removing cookies, or we're just shifting to another way of tracking people? It's making it more difficult for people to understand what they're using to track them. And still, it's interesting that Google is still collecting a lot of data that I don't think they are transparent about."*. Similar to the previous expert's statement, he also does not see any privacy-focused solution that could become an industry standard, instead, he argues for collecting first-party data on a larger scale.

The last informant, Thomas Bering from Google, surprisingly did not praise FLoC (technology developed by Google) to become the next big industry standard. Bering emphasizes that he is speaking from his own personal point of view and states: *"Personally, I don't think there will be an industry standard, actually is my completely honest answer. I think the standard will be more first-party data. So the standard will be businesses being better at picking up their own data."*. In general, he thinks that businesses will focus more on optimizing their internal systems rather than relying on third-party offerings. He also does not believe that users will notice the implementation of FLoC.

To conclude from these answers, all informants were hesitant towards pointing at only one industry standard since everything is so early in the development and adoption state. Although, they did all point at collecting and utilizing first-party data as a very crucial success factor for businesses, and expressed the importance of offering privacy-first solutions to their users. A general opinion by each of the experts was that businesses cannot fight the change towards a more privacy-centered future. Instead, businesses can adopt the mindset of structuring their value offerings around being privacy-centered. The demands for higher data

privacy standards are not going away anytime soon and the quicker companies adjust their offerings, the better the outcome will be and they may acquire a strong advantage compared to their competitors.

6.2.4 Theme 3: User privacy concerns

When the experts were asked about their experiences with users sharing concerns about any potential misuse of their personal data, the results from the experiment were presented to them. The presented results showcased that the average user is not always willing to share their personal data (email was asked for during the experiment) even though they are promised to receive personalization benefits in return. The findings were explained to the informants as follows: “We conducted an experiment where respondents were asked to share the email with a fictional online shop. So we asked them to share their email and in return, they would get personalization benefits. And the result was that we actually found it to have a negative effect on their willingness to share the information. Why do you think that is?”

Rhys Cater started answering this question by expressing that users, in general, have a very low level of trust towards businesses, especially if they do not know the company behind: *“If you look at the average person. If you talk to a friend who doesn't work in our industry, or parent or whatever, they are likely to treat digital marketing and the internet, especially with regards to this data stuff, with quite a lot of mistrust.”*. He explains that whenever someone uses an online service for free, most of the time they are paying for the service by sharing some of their personal data. He mentions Instagram and Google Maps as examples. The users receive entertainment or practical guidance for free if they give access to become tracked - in which case it would be arguable that the service is not free after all, since data has become the currency that is exchanged. He thinks that people might have declined the offer from the banner because the willingness to accept lies within the positioning of the messaging, how the value is presented, the phrasing, lack of trust towards the business behind, and potential user suspiciousness of a hidden catch.

When it comes to the business point of view, represented by Morten Hansen, he explained a possible reason to why the negative effect was found on the willingness to share data when

personalization is offered in return: *"You probably want it* (personalization)*, but if asked for it, you don't want to say that that's what I want. Because I think you're afraid that you're sharing too much personal data, like it's maybe it's in the wording as well, like it's your personal space. So I don't know if you phrased it differently. But it's also how would you phrase it then, because it is about you specifically as an individual getting this offer."*. He emphasizes that users, himself included, want to receive personalization benefits but are hesitant towards sharing their own data. It potentially lies within the mistrust issue. He explains how the news coverage and investigating journalism on the topic have made the general public scared of what big tech companies can do with their data. He argues that there is a common misunderstanding that personalization is invasive to privacy, whereas he personally appreciates personalization because he can receive a relevant offer at the right time. He emphasizes that companies have to improve delivering the right message at the right timing to succeed with personalization. If the company only offers a discount code in exchange for an email sign-up, it could be risking that the user will opt-out after having used the discount code which is not beneficial in the long run. It is important to keep engaging the users after having earned their data to avoid opt-outs.

The last interviewee, Thomas Bering, argues that Google is trying to be as transparent as possible when it comes to advertisement, although they do not see that the concerns expressed by users match their actions: *"We give a lot of ads transparency, insights, anyone can click on the eye to see why they're being shown this ad, you can do the same on Facebook, you do the same on most platforms. I think the average user doesn't use them. But those of us who are in the business, we think that everyone is interested, to be honest, no one really cares."*. He also expresses that people are very concerned about being surveilled online and are scared that anyone can be watching exactly what they are doing online which is highly unlikely: "Y*ou earn so little of one person. It's only when there's a thousand or a million, then it actually starts to add up. So everyone wants to feel that they're the most important person. And they are important. But ask a big company, what would happen if you took out one of these people? Nothing. So again, this idea of all the big companies can see who I am. We can't either, that option doesn't really exist. But even if I could go in and see what either of you were doing, it wouldn't add any value. It would not make the product*

better or worse, because we cannot tailor products to individual people, we can tailor to groups.". He argues that our experiment showed a negative result because we are not representing a well-established and trusted brand - a fictional store for the experiment can result in a very limited trust from the respondents. Furthermore, he argues that the experiment might not only have been affected by users' privacy concerns but could also have been influenced by the respondents' fear of receiving too much spam.

To sum up the experts' experiences on user privacy concerns, there is a common agreement that users are concerned due to lack of trust for businesses. There has been a lot of media coverage on the topic which made the users hyper-aware of their data sharing. They do not always know or understand what the businesses are able to do with their data, therefore they would rather not share too much. Educating the users and establishing trust is crucial for businesses to overcome this obstacle of user concerns. The experts all agree that personalization is important to offer users because even though users are not directly expressing the need for it, they still expect personalization.

6.2.5 Theme 4: Critical view on legislation and privacy trends

Unrelated to any specific question we had prepared, all the experts individually expressed their critical views on the current legislation and areas where privacy trends have gone too far.

Rhys Cater expresses a concern that too many restrictions for businesses collecting data will hinder innovation: *"We see that data brings enormous advantages and allows us to do things faster and more effectively in many cases when it's used correctly. So it's not to say that privacy isn't important. Of course it is. But it shouldn't come at the expense of being able to do great things with data."*. Although, he is positive that businesses will find their own way of utilizing collected data and create proper results, even though data can be limited.

He believes that the legislation will change and become more nuanced in areas like cookie consent. He does not believe that the current cookie pop-ups create value for the users, rather they can provide a bad user experience and annoy them. He argues that the intention behind

the cookie law is right, however, the execution is flawed: *"I think we'll look back on this time and this legislation, and hopefully, it will develop a lot to become more nuanced. I think if you look at stuff like cookie laws, it's a bit silly. The whole kind of thing like cookie notices on every single website, like it's a horrible experience. I would argue that it makes people's experience worse, not better. It's obviously very well intentioned, it has good results in the sense that it forces people to reflect on how they are using customer data. But from a usability perspective, these laws are pretty bad, I think"*. Morten Hansen expressed the same opinion on cookie laws: *"Both from a professional and a personal point of view, I think it's super annoying that you have to accept cookies, privacy policy all the time. I think there will have to be, in the next couple of years, I think there will be something about that. Because that constant popping up being asked about that... I'm sure that consumers are a bit fed up with that."*.

The last expert, Thomas Bering, added that users might not be as concerned with their data privacy as they are with their data security, and some users might mix up these two terms. Data security revolves around the protection of data to not fall into the wrong hands, e.g. he mentions banks leaking information as a security breach. Data privacy revolves more around preventing surveillance than securing data.

6.2.6 Theme 5: Advice for businesses adapting to privacy-first standards

The very last question we asked the experts to sum up the discussion was: "What is your advice for businesses trying to adapt to these privacy-first standards?"

Rhys Cater started answering the question by emphasizing the importance of taking data privacy seriously. He often advises clients on this matter and educates them on how to communicate with their customers properly in order to earn their trust and thereby, their data. He expresses the importance of involving the whole organization in the privacy debate, not only leaving it to the marketing department. Data privacy should be integrated into all aspects of an organization. He expresses the urgency of dealing with the issue now, acting sooner rather than later, and going over and above the minimum requirements: *"It's pretty clear which way the wind is blowing, these laws aren't going to go away in the next years. If you*

look at a five year horizon, it's probably going to get stricter. Maybe if you look at 10 years away, things might start changing a little bit, but by that time, it's so far away, it's impossible to plan for. So what you should plan for now is for privacy to be on the agenda for like, the next few years, pretty highly.". He argues that businesses are expected to cater to their customers, not the other way around, and they should be considering privacy of their customers as a top priority because it might be a unique value offering that could outcompete their competitors: "*As a business, it's not a great look to be just doing the minimum possible in this area. Soon enough customers will expect it from businesses. It will be probably a differentiator when it comes to whether people choose to buy or not from a company"*.

The business representative, Morten Hansen, makes a similar point to Rhys Cater's comments. His advice is to follow the data privacy guidelines strictly because customers express that they care about how their data is being used. He mentions the importance of building trust and being transparent: *"I think reputation is a thing. Otherwise, being transparent as a company, super important. But that's always been my opinion also in terms of having a trustworthy brand."*.

Lastly, Thomas Bering, expresses that businesses need to accept the changes happening and adopt a future-oriented mindset. The demand for data privacy is not going away anytime soon, he argues. Businesses need to be more mindful of the data they are collecting and avoid being "data-hungry", as he explains: *"We still see some businesses sort of sitting back and saying: "No, no, we have all this data. And we have to keep doing this {...} But how can we keep tracking this way?". And I just have to say: "Well, you can't {...} It's like saying you still want to ride your horses on the motorway, but you're just not allowed to because we have cars now. And so, roll with it."*. He explains that his clients are very focused on collecting as much data as possible about their users, but often they do not know what to look for or how to use the data properly. He argues that businesses need to be sure about what they are aiming at collecting and why: *"I have genuinely had that request from a large Nordic customer. "We'd like the search data of every single customer who visits us from your site". And my first thought was: "Why? What are you going to do with it?". And they couldn't really answer but they're like: "That would be really valuable for us to have". No, it wouldn't."*. In

general, his advice is to be more mindful of which data is collected, instead of asking the user for too much.

To sum up, the experts' best advice for businesses trying to adapt to the new privacy standards, building trust, and taking data privacy seriously are two very important topics. The changes are not going away, so it is best for businesses to adapt sooner rather than later.

7.

DISCUSSION

REFLECTION ON THE FINDINGS, LIMITATIONS AND FUTURE RESEARCH RECOMMENDATIONS

7. Discussion

As earlier mentioned, prevailing digital marketing practices are being disrupted by (1) growing user concerns about how their data is being collected and used, (2) increasing privacy regulations, and (3) restrictive practices employed by advertising platforms and technology firms. These changes are disrupting various stakeholders, including users, businesses, agencies, and advertising platforms - this research engages in discovering the perspectives of each stakeholder with the main focus of how businesses should adapt to this new privacy era. Currently, marketers that already have to be proficient in business strategy, creativity, innovation, and technology have to add another increasingly important skill of navigating in the field of privacy since it significantly influences not just legal compliance but overall marketing strategy and the effectiveness of advertising. Thus we raise a question - *how can businesses prepare for a privacy-first future to become digital marketing frontrunners?* To examine the problem and answer the research question we have conducted both quantitative (user survey with experimental elements) and qualitative studies (expert interviews).

7.1 Reflection on the findings

In this section, a reflection on three major pillars of the research results is presented. These pillars consist of the biggest trends and shifts in the fields of digital marketing and privacy, user willingness to share their personal information and recommendations for businesses on how to best navigate in current times and future-proof their marketing strategies.

7.1.1 Biggest shifts in the fields of marketing and privacy

It is essential to examine the biggest changes that have been occurring in the field of marketing and privacy to bring clarity to the complex, uncertain, and rapidly changing environment. The major shifts are defined by three categories - growing user concerns about data privacy, increasing privacy regulation, and practices employed by the biggest advertising platforms and technology firms. These factors are interconnected and have a significant impact on both the current and future marketing landscape.

7.1.1.1 Growing user concerns about their data privacy

Growing user concerns about how their data is being collected and used is surely one of the main drivers of change in the field of marketing and privacy. The survey results show that general awareness about privacy issues online and concerns about personal privacy are relatively high. 86% of the respondents agreed that the internet causes serious privacy problems, while 64% of them were currently concerned about their own personal privacy. Regarding *transparency*, 82% of the respondents agreed that it is important to be informed about the purpose for which the site wants to collect information from them as users. Even though *general privacy concerns* and *transparency* did not have a significant impact on user *intention to provide their personal data*, as standalone measurements they represent user awareness in the privacy area.

The new era of privacy arguably categorized users into two types - those willing to share their data with marketers (buffs) and those who deny access to their personal information (ghosts) (Thomaz et al., 2020). This is enabled by an increasing number of options that allow users to opt-out of data collection by default (e.g. removal of third-party cookies, Apple iOS 14.5 update, etc.). User concerns about privacy and technological options allowing them to stay out of sight of marketers, at least to some extent, has significant implications on marketers since a chunk of user activity online might not be visible, thus any kind of attribution and communication becomes more difficult to conduct.

However, it is important to note that according to the interviewed experts, the average user does not care about the technical part of privacy, they do care about what they see and what affects them directly, such as retargeting ads following them around the internet. All of the interviewees agreed that changes in user tracking such as FLoC, Apple iOS 14.5 update, or removal of third-party cookies will not be very noticeable to the user and that it is not the object of concern for the users overall. Rhys Cater and Morten Hansen argue that potentially by removing cookies, advertising platforms are just shifting to new ways of tracking people making it more difficult for users to understand what advertisers are using to track them. Rhys Cater puts the new technological advancements of tracking in perspective by saying that if consumers and lawmakers wanted to end up exactly where we are today but without

using third-party cookies it would be a great solution. However, to the expert's opinion, users mostly care about who has access to their data and what it is used for. Thus it is debatable if these technologies are going to solve the essential problems related to user privacy concerns.

7.1.1.2 Increasing privacy regulations

The General Data Privacy Regulation (GDPR) set a worldwide precedent on how private user data can be regulated. Other countries have been following European suit and have either established or are looking into establishing regulations - state of California (CCPA), Australia (Privacy Amendment), Brazil (LGPD), India (PDPB), and other countries already have their local variants of general data protection legislation. More regulations are being developed representing a very clear trend - privacy regulations worldwide are increasing. Such regulations not only made businesses pay more attention to privacy, collection, and processing of user data but also drew user attention to the rights they possess over their personal data. The survey findings show that users indeed care about transparency aspects such as how long their data will be stored and for what purpose it will be collected, signifying that essential GDPR principles are deeply rooted within user expectations and demands.

In addition, directives such as the ePrivacy directive (EDP) or "the cookie law" that will be replaced by ePrivacy Regulation (EPR), supplement GDPR and address crucial aspects of electronic communications and tracking of internet users. However, even though EDP's goal is to protect online privacy, which is essentially beneficial for the user (Electronic Privacy Information Center, n.d.), the directive arguably could be impacting user experience in a negative way according to the interviewed experts. The experts argue that constant cookie consent pop-ups are "annoying" and that laws will have to change to take not only user privacy but also user experience into account. Rhys Cater suggests that in five to ten years' time legislation will develop to become more nuanced and that there might be a movement trying to push alternative models for establishing legal grounds for data collection and processing. Indeed, the *privacy fatigue* phenomenon has a significantly negative relationship with users' *willingness to provide personal data* according to the quantitative findings from this research.

The constantly evolving field of privacy regulation has a major impact on marketing jobs. According to Rhys Cater, disciplines that marketers have to be good at keep increasing and it is one of the greatest challenges for marketing managers. In addition to being well versed in technology, strategy, and communication areas, they have to understand and follow rapidly evolving regulations that are often up to interpretation without much precedent in trials, creating a relatively gray area and complexity. Cater underlines that there still will be a lot of turbulence and uncertainty in the few years to come and that the key people in companies will be those who can bring direction in such a challenging environment.

7.1.1.3 Practices employed by advertising platforms and technology firms

Regulations have pushed browsers to discontinue third-party cookie tracking, which will be terminated on all major platforms by 2022 (Bump, 2021). The three interviewed experts agree that such a change will require adjustment. Thomas Bering suggests that agencies might have a bigger role to play in regards to pulling and processing data from different sources because various user touch points are going to be increasingly disjointed. Moreover, Rhys Cater assumes that it is unlikely that we are going to converge around one standard for an ad-supported web that everyone is happy with anytime soon.

Advertising platforms, e.g. Google, as well as technology firms, e.g. Apple, have been developing their own user privacy-enhancing solutions that have been widely discussed in the previous chapters. Google's FLoC technology, a machine learning mechanism that will replace cookies and group users into cohorts that marketers will be able to target, is meant to prevent potential individual user identification and tracking, thus providing more privacy. Expert Rhys Cater agrees that such technology is a step forward, however, the expert admits that FLoC enables user data to be used for the same purpose as it was with cookies just in a slightly different way. From a technology firm side, Apple iOS 14.5 update, which disables user tracking cross-apps without users proactively opting in, has drawn the most attention recently. Apple's decision has caused turmoil for advertisers, especially small to medium-sized businesses that do not have big pools of first-party data thus are reliant on targeting possibilities offered by advertising platforms (Kafka & Morrison, 2021). Such advertisers are also usually tight on marketing spend thus they find the return on ad investment crucial

(Federighi & Stern, 2021). Facebook has been one of the most vocal opposers of the iOS update since it will have a noticeable impact on insights and targeting possibilities for their clients. Based on the current trends it is likely that more privacy-first technologies will be developed and utilized by advertisement and technology firms.

The incentives to develop privacy-first technologies by the platforms emerge from different reasons. Some argue that big tech firms are trying to capitalize on privacy, gain an advantage compared to their competitors by positioning themselves as privacy-focused in the eyes of consumers and legislators (Kafka & Morrison, 2021). However, none of the experts personally believe that there is a clear industry standard that one of these technologies will enable. They doubt that, for example, Apple's Safari and Google's Chrome browsers will come together to find a solution that both parties would be willing to implement due to the different incentives that the businesses have. Rhys Cater believes that such inconsistencies between various industry players will make marketers operate in a fragmented environment for a while, where people will be using different browsers or operating systems that will provide advertisers with varying levels of insight and reach. Based on the current digital marketing and legal landscape, experts deem that the closest adoption to a standard will be companies improving in first-party data collection and utilization.

7.1.2 User willingness to share their private data

To recap, during the survey users were randomly shown one of four banners representing a different value proposition (hedonic, utilitarian, personalized, or generic) and asked about their willingness to share their personal data (email). It was found that *personalization* has a significantly negative effect on *intention to disclose personal information*, while other variables had no significant effect. In regards to user perceptions, it was found that only the *value of information disclosure* and *privacy fatigue* had significant positive and negative effects on the dependent variable, respectively. The aim of this section is to dwell deeper into the reasoning behind such findings.

7.1.2.1 User approach towards personalization value proposition

The finding that *personalization* has a negative effect on *intent to disclose personal information* sparked curiosity to discover the potential reasoning behind it. According to the literature review, a personalization privacy paradox might be one of the reasons. According to Xu et al. (2011), users might be willing to give out as little information as possible even if they value personalization or expect to receive personalization benefits. Some authors suggest that users might be willing to participate in the personalization privacy trade-off depending on the customers' trust in the firm (Davenport et al., 2020 & Thomaz et al., 2020). Additionally, personalization might not be beneficial in every situation and context, e.g. Sheng et al. (2008) argue that the intention to share personal data increases in emergency contexts (situations that are time-critical, location important, and where user identity is needed).

During the interviews, the experts were asked to share their experience and knowledge on how users react to personalization to find out if personalization should even be the aim of advertisers. All of the experts agreed that an important prerequisite is consumers' trust in the company. Rhys Cater believes that the level of consumer trust is generally low and people might not feel that they are getting enough in the personalization privacy exchange. This is in line with the quantitative analysis results, which showed that users are willing to give out their data if the benefits are sufficient. According to Thomas Bering, another sign of user mistrust might be the fear of spam, where users do not believe that they will get information or benefits that are relevant enough at a frequency that they are comfortable with. Additionally, the interviewed experts described trust as familiarity with the company and the context. They also mentioned the importance of wording in the value proposition offering. During the interview with Morten Hansen, he came to a conclusion that marketers might be biased towards the keyword "personalization" in their messaging as they see it as a goal of their communication and as a beneficial thing for the user. Meanwhile, users might have an entirely different perspective on the keyword, which might raise the previously discussed mistrust issues and fear of spam. Thomas Bering noted that small tweaks in the copy that people might not even be conscious of can make a difference. As an example, in addition to offering personalization, a marketer might add keywords such as "organic lifestyle" or

“minimalistic lifestyle” that would each bring specific value to different segments. Bering further argues that it might be more challenging to communicate the value proposition rather than deliver it. The experts reflected that users probably want personalization, which is essentially “getting the right message at the right time”, but might not respond to a personalization offer in an expected positive way. Rhys Cater added to this point, that nowadays personalization is an expected standard - users expect relevance. Thus, other factors such as trust and convenience might be much more powerful tools that incentivize users to share their private data.

7.1.2.2 User perceptions of privacy

In addition, users were asked to answer questions related to their perceptions of privacy in the survey. It was found that users are highly aware of privacy issues online and are concerned about their privacy but it does not affect their willingness to share their personal information. Reviewed literature suggested that privacy beliefs stated by users and their actual behaviors might differ (Rainie & Duggan, 2015). One of the interviewed experts, Morten Hansen, suggested that increased awareness in the privacy area might be due to GDPR, other user privacy-protecting measures such as the Apple iOS 14.5 update, investigative journalism into privacy policy misconduct and whistleblower scandals that have gotten a lot of traction in the news. Rhys Cater notes that in the area of privacy most people care about who has access to their data and what it is used for. Thomas Bering argues that users do not think too much about their personal privacy in reality when seeing ads - they care about the content they are reading or watching and if the ad that pops up is not relevant it is simply being ignored. According to the expert, in regards to privacy scandals where data has gotten into the wrong hands, especially if it was such sensitive data as bank details, personal impact could be felt. However, he is worried that such problems conflate with general privacy concerns when users cannot distinguish between very different types of privacy concerns such as someone breaking into one’s bank account and someone knowing one's interest in a particular shoe category. He argues that major data security scandals do not represent the problem with internet privacy. Lastly, Thomas Bering brings individual user identification risk into a broader perspective saying that unless one is a generally important person in the public eye, such as a celebrity, no one really wants to identify a specific individual even though people

tend to feel that their individual data is highly important. According to Thomas Bering, data makes sense and has value to most companies when it is clustered into bigger groups of people. This finding signifies that there is minimal interest by both first and third parties to identify individual users which questions the validity of this specific user privacy concern.

7.1.2.3 User approach towards transparency

Similarly, users greatly value transparency, specifically being informed for what purpose their data is being collected, and for how long it will be kept, however, it has no significant impact on user willingness to share their personal information. This finding is supported by authors from the literature review, e.g. Katwatzki et al. (2017) found no indication that providing transparency features facilitates individuals' information disclosure. From the perspective of the Google representative, Thomas Bering, transparency is already there on most of the platforms, e.g. everyone can easily check why they are being served a certain ad, but the average user does not use these functions, signaling that users might be stating their interest but not caring enough in reality. Bang & Olufsen representative Morten Hansen contrasted with Thomas Bering saying that Google still collects a lot of data that they are not transparent about or that users are not aware of. He added that personally, he would prefer platforms being more transparent, providing users with full information on what is being tracked, and allowing users to easily opt-out. In line with the findings of the survey, Thomas Bering underlined the importance of clearly disclosing the purpose of information collection - there is a great risk related to businesses asking for unnecessary additional information to deliver a value proposition. Such findings suggest that transparency is an important factor that users demand, however, it is not critical when deciding whether they will share their personal information.

7.1.2.4 User approach towards privacy fatigue

It was found that the *privacy fatigue* variable had a significant negative effect on users' *intention to disclose their personal information*. According to Choi et al. (2018), *privacy fatigue* has a stronger impact on privacy behavior than *privacy concerns* do which has proven to be true by this research. Authors also suggest that *privacy fatigue* potentially can have a long-term impact on online vendors and policymakers and that policymakers should continue

adapting policy to accommodate both user privacy protection and convenience in order to combat *privacy fatigue*. The *privacy fatigue* topic came up during interviews with Morten Hansen and Rhys Cater, who both noted the current situation with cookie banners, where one has to select their preferences every time they are visiting a new site, provides a poor user experience, is annoying, and causes exhaustion. Both interviewees elaborated that they would expect some kind of changes in this area, while Rhys Cater even called it a potential future big movement that will push alternative models for legal grounds.

7.1.2.5 Finding the right value proposition

Finally, the perceived *value of information disclosure* variable has a significantly positive relationship with users' *intent to disclose their personal information*, thus it can be concluded that if businesses find relevant value propositions and successfully convey them to the consumer, they should be able to collect first-party data. According to Distler et al. (2020) users' intent to disclose personal data depends on how *private* or *sensitive*' the type of data shared is perceived by the users - in our research respondents were asked to only submit their email thus potentially it could be qualified as non-sensitive data. Moreover, researchers suggested a theory of privacy calculus, which measures people's intention to disclose personal information based on their goal to maximize the positive and minimize the negative consequences. Our finding proves that the privacy calculus is indeed a factor that businesses and advertisers should account for. All of the interviewed experts strongly supported the idea that users would be willing to disclose their private data if the value received in exchange is sufficient. It does not mean that there is a one-size-fits-all value proposition, it depends greatly on the context, type of business, and preferences of its customers. Thomas Bering argues that even personalization could have a positive effect in certain contexts, e.g. when users interact with a brand they are already familiar with and trust will act in their best interest.

7.1.3 Recommendations for businesses

The following section answers how companies can adapt to a privacy-centered future and become digital marketing frontrunners. Furthermore, it explains how businesses could adapt and excel in the current privacy-dominated marketing landscape. Recommendations are

drawn by combining desk research (extensive literature review, media publications, and reports) and primary research (quantitative and qualitative analyses).

7.1.3.1 Developing a privacy-first strategy

As the interviewed expert Rhys Cater said: “It's pretty clear which way the wind is blowing”. The relevancy of data privacy is not going away in the foreseeable future thus businesses “have to accept it”, prioritize it greatly on the business’s agenda, and “follow privacy rules to the strictest terms”. Rhys Cater underlines that businesses must make sure to “take it seriously” and not only adapt to the legal requirements but go “above and beyond" of what is required. Both the industry trends and the primary research show that data privacy is under the consumer radar and that companies who are not compliant are risking losing consumer trust. The experts predict that customers will prioritize interacting with and buying from those companies that make it easy for them to control their own data, that do not ask for too much unnecessary information and deliver sufficient value in return for the data collected. This is in line with our survey findings, which prove that *privacy fatigue* has a significantly negative relationship with user *intention to provide their personal information*.

7.1.3.2 Mindset change and cross-department collaboration

Changes in the digital marketing landscape require a mindset change of business managers. Expert Rhys Cater observed that there is “a lot of fear and resistance to change your businesses" since businesses are used to working in ways of data abundance. All experts recognize that it is not easy to adapt to the strictest data privacy terms and lose vast amounts of information but it is necessary to take the step. Expert Thomas Bering elaborates that the biggest challenge is facing the unknown, since moving away from being able to measure everything and target precisely rips away the entire foundation from the businesses. He advises businesses to just accept the changes: “It's like saying you still want to ride your horses on the motorway, but you're just not allowed to because we have cars now”. Another important aspect of mindset change is involving other departments since organizational change is required in order to develop and adapt privacy-first strategies. Rhys Cater elaborates that it is critical to have a cross-functional senior working group - it is not just about the digital marketing department anymore. To make this work, representatives from

legal, marketing, business intelligence, and senior leadership have to be convinced that the ways in how businesses collect and utilize data are changing and that it is not one employee's or department's job to adjust to. If they succeed, they can possibly even benefit from the changes. Thomas Bering adds that without senior leadership on board none of this would work. Research conducted by Google and Deloitte, where the researchers analyzed clients that have started to implement privacy-first strategies, is in line with the experts' recommendations. According to the researchers, C-suite executives should be the ones who start defining transformation plans, while all teams have to be united around the common vision implementation (Bartolletti, Ingrey, 2021).

7.1.3.3 Exploiting opportunities

On another note, experts agree that these changes can also bring opportunities. According to Thomas Bering, companies will become better at collecting first-party data, meaning that they should improve at engaging consumers, finding ways to deliver value, and build trust in order to make users share their data. Bering believes that companies will be more "focused internally in the business, rather than third party offering", e.g. they could segment customers in their CRM databases and customize value propositions including messaging to make the most out of the data that users trustfully shared with the company. He also adds that setting benchmarks for acquiring first-party data is important and that businesses can utilize the insights they have gotten by growing their first-party data pool and plan subsequent strategies for the future. Morten Hansen suggests that first-party data should be utilized by marketers as much as possible and that it will play a big role in precision marketing, which is a marketing technique used to retain, cross-sell and upsell existing customers (Peppers & Rogers, 2004). Research conducted by Google and Deloitte supports the experts' opinion that moving beyond compliance and becoming better at first-party data collection can hold significant benefits (Bartolletti, Ingrey, 2021). They found that such clients started seeing more innovation and experimentation that led to new ways of engaging individuals towards longer-lasting relationships with customers (Bartolletti, Ingrey, 2021). Researchers declare that first-party data collection based on customer's needs and expectations makes the value exchange "more meaningful and based on trust" (Bartolletti, Ingrey, 2021). The survey findings of this research show that users are *willing to provide their data* and even overcome their *general*

privacy concerns if enough value is delivered, thus supporting the idea expressed by experts and previously discussed research that companies can indeed obtain user data if they work for it. However, Thomas Bering draws a point that businesses should not be greedy with data by believing that they should collect as much as possible - this could significantly degrade user trust and does not assure that crucial insights can be drawn from it. Lastly, Rhys Cater wants to remind businesses that simply having first-party data is not enough, it has to be gathered with the right legal basis to be used for marketing purposes.

7.1.3.4 Collecting first-party data

As the findings deem first-party data collection as crucial, how should businesses collect it? To answer this, a survey was conducted where it was analyzed what factors would increase user *intention to provide their personal data*. Part of the survey was an experiment where users were randomly assigned a banner with different value propositions or, in other words, incentives. We found that *utilitarian* (a 10% discount), *hedonic* (a free branded item as a gift) and *generic benefits* (no distinctive value proposition identified) had no effect on *user willingness to provide their personal data*. However, *personalization* benefit had a significantly negative effect. To understand such phenomena, literature review and expert interviews were utilized in order to find any other important factors to consumers than solely direct incentives, or if any prerequisites have to be in place for the incentives to work. All experts agreed that building trust is the most essential prerequisite. It signals that there is no fast and easy path to gather lots of first party data - it has to be a strategic process which involves many user touchpoints. As an example, Morten Hansen suggests that branding activities, e.g. storytelling, are very influential on user decisions to interact with companies and eventually make a purchase. Furthermore, Hansen points out that personalization is rather a lower funnel activity, meaning that a sufficient data pool already has to be present in order to deliver the benefits. Otherwise bigger pools of audiences need to be targeted, where branding activities that increase awareness could be especially relevant. He also suggests that trust could be built utilizing reviews and recommendation sites and focusing on customer service excellence. Thomas Bering argues that if consumers would believe that personalization saves time and brings convenience they would not doubt benefiting from it and providing marketers some of their data. Lastly, all of the experts talked about the

importance of messaging and behavioural economics. Even little tweaks in messaging for the same value proposition can bring different results thus experts recommend testing as much as possible to find the best way of collecting first-party data.

Additionally, the digital marketing trends analyzed in this research show that despite new regulations and other limitations, such as Apple's App Tracking Transparency, major advertising platforms will remain relevant to the advertisers - they will still be generating vast amounts of user data despite any of the roadblocks. Technologies developed by these platforms, e.g. Google's FLoC, are steps towards more user privacy in some sense, however, they will not fundamentally change how users are being tracked and targeted yet. Companies that do not have enough first-party data will be dependent on these platforms to generate leads, while companies that do have certain pools of first-party data will be using machine learning algorithms offered by the platforms to generate more leads that are similar to those in the first-party data pool. Thus major advertising platforms are very likely to be utilized by companies of all sizes and industries due to the large user pools that advertisers can tap into and due to the machine learning technologies that allow advertisers to make the most out of their own first-party data pools.

7.1.3.5 Importance of context and testing

All in all, there is no straightforward recipe for how businesses can best adapt in the privacy first era and collect first-party data. As the expert Thomas Bering says "We're going to have to take this next step to find out what happens here. And the companies don't have the answers. The agencies don't have the answer. Google doesn't have the answer. Apple doesn't, Facebook doesn't, no one has the answers.". Personalization is apparently not the golden standard as marketers seem to think, and it is not the single answer to solving first-party data collection challenges and guaranteeing attractive benefits to the consumers. All experts underlined the importance of trust and context when setting up a first-party data collection strategy. Even though they are sceptical about incentives as standalone value propositions, they encourage businesses to strategically test different marketing mix combinations and value propositions for different segments. Morten Hansen reflects that offering a discount could maybe make sense for a FMCG (Fast Moving Consumer Goods) brand, but luxury

brands should never utilize that and instead focus on excelling at user experience and customer service. Thomas Bering recommends watching competition closely and asking oneself why the competitor is getting customers that their business is not, while examining the value they are offering. Moreover, it is important to improve strategies of engaging those who willingly shared their personal data or opted in - there is always a chance that consumers will eventually opt out if their needs are not met. To figure out answers along the way, Morten Hansen recommends managers asking themselves "What is your goal for your brand? What makes sense for your brand?" to get on the right track.

7.2 Limitations and future research recommendations

Critically reflecting on this research, there are certain factors that are worth taking into consideration as they might have had influence on the results. Firstly, the experiment and overall quantitative research was based on the variables that were defined in the literature review. Naturally, there are countless factors that influence *user intention to share their data* thus this research was narrowed down to a few that were deemed to be the most important and feasible to investigate. As an example, such factor as *trust* was mentioned in the reviewed literature and during the discussions with the experts. It was found that the variable is an important prerequisite for *user intention to share their data*. However, it was not investigated in a quantitative way since the focus was narrowed down to specific instant benefits provided for a newsletter sign up and general user perceptions. Variables that would relate to the fictional e-commerce shop, such as *trust, branding, reputation* and similar, were not taken into account for the quantitative research (however, it is important to note that they were discussed in the qualitative part). Secondly, the fictional e-shop was in the fashion category, thus it could be argued that the category itself might have influenced the users' willingness to subscribe to a newsletter due to personal preferences. Another potential limitation of the experiment could be the wording in the banners. The experts, who participated in the qualitative part of the research, noted that from their experience even little tweaks in the value proposition text can have a great impact on user response. There are many ways in which each of the four value propositions that were chosen could be put in writing and it is acknowledged that copywriting could be one of the limitations. Lastly, as one of the experts Thomas Bering noted, the banner experiment could be a rather simplified way to test a

relatively complex problem. Indeed, user *intention to share their data* is a nuanced problem that could be researched further, however, this experiment was chosen to best fit the scope of this research and could potentially benefit other researchers aiming to investigate the phenomenon further.

In regards to the qualitative part of this research, certain limitations must be acknowledged as well. A limited number of experts were interviewed due to the scope of the research. It might not be a significant limitation overall, since most of the points that experts provided were similar or comparable insights signaling data richness. However, it must be taken into account that even though interviewees represent different stakeholder groups (agency, business and advertising platform), all of them are high profile experts working in relatively large companies with significant budgets and access to legal, IT, BI and other qualified workforce which is helpful when navigating the complex privacy-first marketing landscape. It might be beneficial to interview marketing managers representing SMEs (small and medium-sized enterprises) to find out their perspective on the current digital marketing and privacy related challenges.

Finally, there are certain limitations that were elaborated in the methodology section. To recap, the survey was distributed by employing voluntary response sampling based on ease of access which may result in some bias - potentially this might have attracted respondents with exceptionally strong opinions that might not be representative of the general population or acquaintances who might be somewhat similar demographically. Regarding the expert interviews, it can be questioned if other researchers would come up with the same results and if the semi-structured interview manner, whereas certain problems were already identified in the questions, had influence on respondents' answers. However, these biases concerning both quantitative and qualitative approaches were mitigated by carefully choosing the formulation of questions and avoiding any kind of leading questions.

This thesis could serve as inspiration for a variety of potential future research topics. Overall, the marketing and privacy area should be continuously researched since legislation, technology, and user perceptions keep evolving. Moreover, the importance of context was

highlighted in this thesis, signaling that results might differ depending on the industry and type of business. Further research examining users' *intent to share their data* in different contexts followed by specific recommendations for businesses in those contexts would be beneficial. Since it was found that users are willing to provide their data if they do get sufficient value in return, it could be the basis for researchers further examining what value and benefits could incentivize and engage users. Lastly, researching how to mitigate the factors that might make users reluctant to share their data could be valuable.

8. CONCLUSION

8. Conclusion

Privacy is an increasingly relevant topic for the digital marketing industry due to growing user concerns regarding personal data, privacy regulations, and restrictive practices employed by both advertising platforms and technology firms. The complexity of the environment for digital marketers is growing, thus the main objective of this thesis is to examine how businesses can prepare for a privacy-first future to become digital marketing frontrunners. To develop the recommendations, primary quantitative (survey with experimental elements) and qualitative (expert interviews) research has been conducted in addition to extensive desk research. In order to answer the main research question, current privacy trends in the digital marketing industry are explored, including what factors lie behind these trends. Furthermore, it was researched what potential influences would increase users' willingness to share their data with companies.

The digital marketing industry is currently being transformed by various user privacy enhancing solutions such as differential privacy, Google's FLoC-technology, Apple's App Tracking Transparency, termination of third party cookies, privacy-first internet browsers, etc. According to the interviewed experts, it is not likely that a common industry standard for privacy will be established anytime soon due to different incentives that various stakeholders have when developing and implementing these solutions. The factors behind the increasing demand for privacy-centered digital marketing solutions stem from increasing privacy regulations worldwide, legislative scrutiny over big tech firms, and media coverage on users' personal data related misconducts. Subsequently, these factors have been drawing user attention to the rights they possess over their personal data. The importance of first-party data collection by companies will keep growing, since the current tendency clearly indicates that users will continue gaining more control over sharing their data with companies. Thus, we developed seven hypotheses with two sets of independent variables, namely *content of value offerings* and *user perceptions*, that could theoretically have an effect on user *intent to share their personal data*. Three of the hypotheses were accepted - it was found that *personalization* as a value offering and *privacy fatigue* as user perception are negatively related to users' *intent to share their personal data*. However, *value of information disclosure*

is positively related to users' *intent to share their personal information*, indicating that if businesses create relevant value propositions and successfully convey them to the consumers, they should be able to collect first-party data. The rejected hypotheses showed that *hedonic value offering, transparency and general privacy concerns* do not have a significant relationship with users' *intent to disclose personal information.* These findings indicate that although users declare to be concerned about their privacy and personal data, it might not impact their decision of opting-in and sharing their data.

Three experts in the field of digital marketing and privacy were consulted to deep dive into the observed trends, quantitative findings, and to define recommendations for businesses. The experts underlined that privacy will remain relevant in the foreseeable future, thus businesses have to take it seriously and approach it strategically. In order to develop a privacy-first digital marketing strategy, a mindset change is necessary - it can be a challenge to embrace uncertainty and overcome the urge of maintaining old ways of performing marketing that are based on abundant, timely, and rich consumer data across channels. Moreover, the strategy should be built and executed as soon as possible. The outbreak of COVID-19 caused an accelerated digital transformation across many industries, while consumers turned to online shopping at a record rate. This increase in online shopping behavior is expected to continue after the pandemic as well. Marketers should secure their business's competitive position by becoming one of those 30% of marketers who are currently collecting and integrating data across channels, or, if relevant to the business, by becoming part of the 1% who are using first-party user data to deliver a fully cross-channel experience for customers (Boston Consulting Group, 2020).

Moreover, cross department collaborations and C-suite management involvement is necessary to adapt to the changes. Everyone has to be on board when building a privacy-first strategy with first-party data collection as the core objective. Businesses will be forced to explore, test, and innovate to deliver value propositions that demonstrate the benefits of sharing personal data and engage consumers in a meaningful way to build longer lasting customer relationships. However, there is no single answer on how to achieve that - as our quantitative research demonstrates, personalization, a common goal for marketers, might

have a negative effect on the users' decision to share their data. Finding the right value proposition for a certain business context and customer segment should be a continuous process of testing since consumer expectations and demands might change over time. Furthermore, it is emphasized by the experts that businesses should be mindful of the type of data they collect. There should be a clear strategy in place for exactly what user information is needed and it should be avoided to ask for anything else than the strictly necessary. The focus should be on maximizing the value of the data rather than collecting as much as possible. All in all, businesses have to think long term when embedding a privacy-first approach into strategies, which is essential to earn consumers' trust and engage them more meaningfully to establish long lasting relationships.

References

AdQuadrant. (2020). What is a Tracking Pixel? Retrieved 2021.05.09 from: https://www.adquadrant.com/blog/what-is-a-tracking-pixel

Apple Developer. (n.d). SKAdNetwork. Retrieved 2021.05.11 from: https://developer.apple.com/documentation/storekit/skadnetwork

Awad, N. F. & Krishnan, M. S. (2006). The Personalization Privacy Paradox: an Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly*, 30(1), pp. 13-28.

Bang & Olufsen A/S (2021). Interim report for the first nine months 2020/21. Retrieved 2021.05.01 from: https://investor.bang-olufsen.com/static-files/5069327d-5031-4d4f-9631-2daecfedc220

Bartolletti, I. & Ingrey, S. (2021). 3 things CMOs should think about when it comes to putting privacy first. Retrieved 2021.05.02 from: https://www.thinkwithgoogle.com/intl/en-154/future-of-marketing/privacy-and-trust/cmo-privacy-first-strategy/

Bietz, M. J., Bloss, C. S., Cheung, C., Rubanovich, C. K. & Schairer, C. (2019). Privacy Perceptions and Norms in Youth and Adults. *American Psychological Association*, 7(1), 93-103.

Bindra, C. (2021). Building a privacy-first future for web advertising. Google Ads & Commerce blog. Retrieved 2021.05.10 from: https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

Boston Consulting Group. (2020). Responsible Marketing with First-Party Data.

Brinkmann, S. & Tanggaard, L. (2015). Kvalitative metoder (2. ed.). Hans Reitzels Forlag.

BroadBandSearch. (n.d). Key Internet Statistics to Know in 2021 (Including Mobile). Retrieved 2021.05.08 from : https://www.broadbandsearch.net/blog/internet-statistics

Bui, Y. (2014). How to write a master's thesis (2nd ed.). Los Angeles: SAGE Publications inc.

Bump, P. (2021). The Death of the Third-Party Cookie: What Marketers Need to Know About Google's Looming Privacy Pivots. HubSpot. Retrieved 2021.05.01 from: https://blog.hubspot.com/marketing/third-party-cookie-phase-out

Cheng, Y. & Jiang, H. (2020). How Do AI-driven Chatbots Impact User Experience? Examining Gratifications, Perceived Privacy Risk, Satisfaction, Loyalty, and Continued Use. *Journal of Broadcasting & Electronic Media*, 64(4), pp. 592–614.

Choi, H., Park, J. & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior,* 81, pp. 42-51.

Church, E. M., Thambusamy, R. & Nemati, H. (2017). Privacy and pleasure: A paradox of the hedonic use of computer-mediated social networks. *Computers in Human Behavior*, 77, pp. 121-131.

Cuban, M. (2017). Data is the new gold. Retrieved 2021.05.02 from: https://www.credit-suisse.com/about-us-news/en.d.rticles/news-and-expertise/mark-cuban-data-is-the-new-gold-201706.html

Davenport, T., Guha, A., Grewal, D., Bressgott, T. (2020). How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science*, 48, pp. 24-42

Davis, K. (2021). Does Google's FLoC alternative to third-party cookies make sense?. Martech today. Retrieved 2021.05.01 from: https://martechtoday.com/does-googles-floc-alternative-to-third-party-cookies-make-sense-246333

Digital Information World. (2020). How Data Privacy Is Changing Online Marketing. Retrieved 2021.04.11 from: https://www.digitalinformationworld.com/2020/01/how-data-privacy-is-changing-online-marketing.html

Distler, V., Lallemand, C. & Koenig, V. (2020). How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. Computers in Human Behaviour, 106.

E-commerce News. (2019). Top 10 online stores in Denmark. Retrieved 2021.03.15 from: https://ecommercenews.eu/top-10-online-stores-in-denmark/

Electronic Privacy Information Center (EPIC). (n.d.). EU Privacy and Electronic Communications (e-Privacy Directive). Retrieved 2021.03.25 from: https://epic.org/international/eu_privacy_and_electronic_comm.html#:~:text=The%20e%2DPrivacy%20Directive%20deals,or%20other%20internet%2Dconnected%20devices.

European Commision. (n.d.). Data Protection in the EU. Retrieved 2021.04.01 from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Federighi, C. & Stern, J. (Hosts). (2021, April 27th). Joanna Stern and Apple's Software Chief Talk App Tracking Transparency [Audio podcast episode]. WSJ Tech News Briefing. Retrieved 2021.04.29 from: https://open.spotify.com/episode/3eukR7rl0IIksM7B23Xb0e

Gan, C. & Li, H. (2018). Understanding the effects of gratifications on the continuance intention to use WeChat in China: A perspective on uses and gratifications. Computers in Human Behaviour, 78, pp. 306-315.

GlobalWebIndex. (2020). Commerce.

Grand View Research. (2020). Digital Marketing Software Market Size, Share & Trends Analysis Report By Solution. Report ID: GVR-3-68038-001-9

Harvard University. (n.d.). Differential privacy. Retrieved 2021.04.01 from: https://privacytools.seas.harvard.edu/differential-privacy

Hayes, A. F. (2018). Process Procedure for SPSS Version 3.5.3 [Computer Software]. Retrieved 2021.04.07 from: www.afhayes.com

InterestExplorer. (n.d.). How Apple's will crumble your Facebook cookie in 2020. Retrieved 2021.03.11 from: https://interestexplorer.io/cookiepocalypse-2020/

Juneau, T. (2020). Digital Marketing In A Cookie-Less Internet. Forbes. Retrieved 2021.03.11 from: https://www.forbes.com/sites/forbesagencycouncil/2020/05/18/digital-marketing-in-a-cookie-less-internet/?sh=3e22677221e2

Kaftka, P. & Morrison, S. (Hosts). (2021, April 28th). Apple vs. Facebook (feat. Privacy) [Audio podcast episode]. Today, Explained. Vox Media. Retrieved 2021.04.29 from: https://open.spotify.com/episode/2MtEePyN7CfqANPPlg0rOA

Karwatzki, S., Dytynko, O., Trenz, M. & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*. 34(2), pp. 369–400.

Keizer, G. (2021). The Brave browser basics: what it does, how it differs from rivals. ComputerWorld. Retrieved 2021.04.11 from: https://www.computerworld.com/article/3292619/the-brave-browser-basics-what-it-does-how-it-differs-from-rivals.html

Koch, R. (2019). Cookies, the GDPR, and the ePrivacy Directive. GDPR.Eu. Retrieved 2021.04.03 from: https://gdpr.eu/cookies/?cn-reloaded=1&cn-reloaded=1

Koetsier, J. (2018). 61% of Americans Will Share Personal Data for Personalized Marketing Communications. Retrieved 2021.04.06 from: https://www.inc.com/john-koetsier/61-of-consumers-will-share-personal-data-for-personalized-marketing-communications.html

Koetsier, J. (2020). Apple Just Crippled IDFA, Sending An $80 Billion Industry Into Upheaval. Forbes. Retrieved 2021.04.11 from: https://www.forbes.com/sites/johnkoetsier/2020/06/24/apple-just-made-idfa-opt-in-sending-an-80-billion-industry-into-upheaval/?sh=610ee54d712c

Koetsier, J. (2021). 8 limitations of SKAdNetwork for mobile marketing measurement. Singular. Retrieved 2021.04.01 from: https://www.singular.net/blog/skadnetwork-limitations/

Kopalle, Praveen & Kumar, V. & Subramaniam, Mohan. (2019). How legacy firms can embrace the digital ecosystem via digital customer orientation. *Journal of the Academy of Marketing Science*, 48.

Kraus, R. (2021). After update, only 4 percent of iOS users in U.S. let apps track them. Mashable. Retrieved 2021.04.09 from: https://mashable.com/article/ios-14-5-users-opt-out-of-ad-tracking/

Kubo, B., Sahk, A., Berendsen, V. & Saluveer, E. (2019). Privacy by design in statistics: Should it become a default/standard?. *Statistical Journal of the IAOS*, 35, pp. 623–631.

Kulpa, J. (2017). Why Is Customer Relationship Management So Important?. Forbes. Retrieved 2021.04.10 from: https://www.forbes.com/sites/forbesagencycouncil/2017/10/24/why-is-customer-relationship-management-so-important/

Lewellyn, A. & Mims, C. (Hosts). (2021, April 16th). Small Businesses Shift Ad Strategies Ahead of Apple iOS Update [Audio podcast episode]. WSJ Tech News Briefing. Retrieved 2021.04.29 from: https://open.spotify.com/episode/21WFDGZsidkuPZjikif4W7

Martin, K. & Shilton, K. (2016). Why Experience Matters to Privacy: How Context-Based Experience Moderates Consumer Privacy Expectations for Mobile Applications. *Journal of the Association for Information Science and Technology*, 67(8), pp. 1871–1882.

McCombes, S. (2021). An introduction to sampling methods. Scribbr. Retrieved 2021.04.02 from: https://www.scribbr.com/methodology/sampling-methods/

Medium. (2018). A Brief Introduction to Differential Privacy. Retrieved 2021.04.11 from: https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b

Miyazaki, A. D. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *American Marketing Association*, 27(1), pp. 19-33.

Morrison, S. (2021). Why Facebook and Apple are fighting over your privacy. Retrieved 2021.04.30 from: https://www.vox.com/recode/22254815/facebook-apple-privacy-ios-14-lawsuit

Newsom, J. T. (2020). Testing mediation with regression analysis. Structural Equation Modeling, Psy 523/623. Retrieved 2021.04.07 from: http://web.pdx.edu/~newsomj/semclass/ho_mediation.pdf

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), pp. 100–126.

Office for National Statistics. (2020). Retail sales, Great Britain: May 2020. Retrieved 2021.04.08 from: https://www.ons.gov.uk/businessindustryandtrade/retailindustry/bulletins/retailsales/may2020

Pariser, E. (2011). The Filter Bubble: What the Internet Is Hiding from You. London: Penguin.

Peppers, D. & Rogers, M. (2004). Managing Customer Relationship: a Strategic Framework. John Wiley & Sons, Inc., Hoboken.

Quinn, K. (2016). Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use. *Journal of Broadcasting & Electronic Media*, 60(1), pp. 61–86.

Rainie, L., & Duggan, M. (2015). Privacy and information sharing. Pew Research Center.

Ramirez, N. (2020). Comparing CCPA and GDPR: 8 Key Differences Between the Privacy Laws. Osano. Retrieved 2021.04.07 from: https://www.osano.com/articles/gdpr-vs-ccpa

Rhodes, L. (Producer), & Orlowski, J. (Director). (2020). The Social Dilemma [Video file]. Retrieved 2021.03.11from: https://www.netflix.com/title/81254224

Richard, M. O. (2005). Modeling the impact of internet atmospherics on surfer behavior. *Journal of Business Research*, 58, pp. 1632–1642.

Rudolph, S. (2018). Why Data Driven Marketing Is Important. Retrieved 2021.04.23 from: https://www.business2community.com/marketing/why-data-driven-marketing-is-important-infographic-02093129

Sanchez, O. R., Torre, I., He, Y. & Knijnenburg, B. P. (2019). A recommendation approach for user privacy preferences in the fitness domain. *User Modeling and User-Adapted Interaction*, 30, pp. 513–565.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2016). Research methods for business students (7th ed.). Edinburgh: Pearson.

Schiff, A. (2020). Why Every Ad Tech Company Must Understand Differential Privacy. AdExchanger. Retrieved 2021.04.21 from: https://www.adexchanger.com/privacy/why-every-ad-tech-company-must-understand-differential-privacy/

Sheng, H., Nah, F. F. & Siau, K. (2008). An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns. *Journal of the Association for Information Systems,* 9(6), pp. 344-376.

Shobeiri, S., Mazaheri, E. & Laroche, M. (2014). Improving customer website involvement through experiential marketing. *The Service Industries Journal*, 34(11), pp. 885– 900.

Simmons, D. (2021). 12 Countries with GDPR-like Data Privacy Laws. Comforte. Retrieved 2021.04.25 from: https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws

Sippel, B. (2021). Proposal for a regulation on privacy and electronic communications. Retrieved 2021.04.15 from: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform

StatCounter. (2021). Browser market share. Retrieved 2021.04.11 from: https://gs.statcounter.com/browser-market-share/all/united-kingdom

TechTerms. (2011). Cookie. Retrieved 2021.04.15 from: https://techterms.com/definition/cookie

Thomaz, F., Salge, C., Karahanna, E. & Hulland, J. (2020). Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science*, 48, pp. 43–63.

Walrave, M., Poels, K., Antheunis, M. L., Broeck, E., Noort, G. (2018). Like or dislike? Adolescents' responses to personalized social network site advertising. *Journal of Marketing Communications*, 24(6), pp. 599–616.

Warc. (2020). Marketers say data privacy is a key theme in 2020. Retrieved 2021.05.11 from: https://www.warc.com/newsandopinion/news/marketers-say-data-privacy-is-a-key-theme-in-2020/43158

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106, pp. 44–52.

Xu, H., Luo, X. R., Caroll, J. M. & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51, pp. 42-52.

Yadav, S. M. & Pavlou, P. A. (2019). Technology-enabled interactions in digital environments: a conceptual foundation for current and future research. *Journal of the Academy of Marketing Science*, 48, pp. 132–136.

Zainudin, A. (2016). 11 Chapter 7 Analyzing the moderating variable.

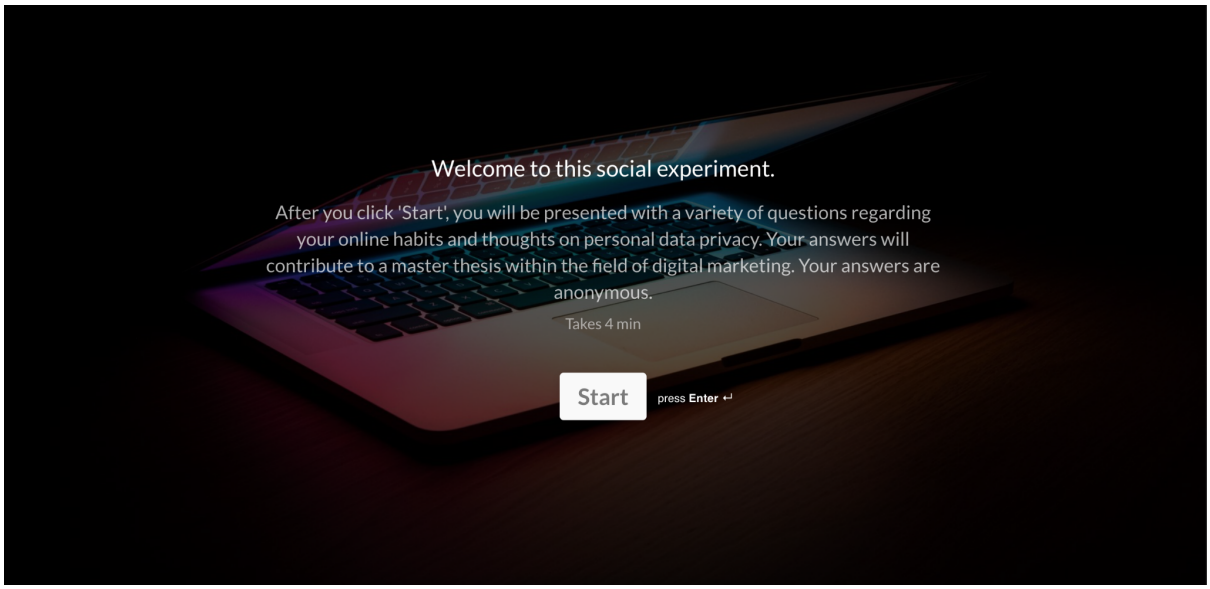
Zhang, X., Guo, X., Guo, F. & Lai, K. H. (2014). Nonlinearities in personalization-privacy paradox in mHealth adoption: The mediating role of perceived usefulness and attitude. *Technology and Health Care*, 22, pp. 515–529.

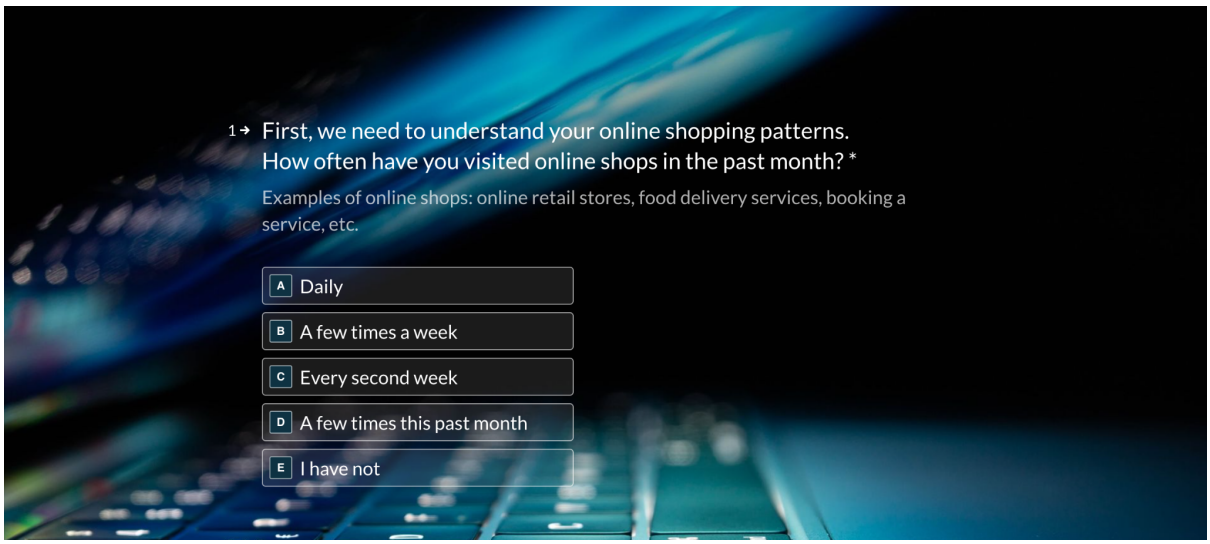
Appendix

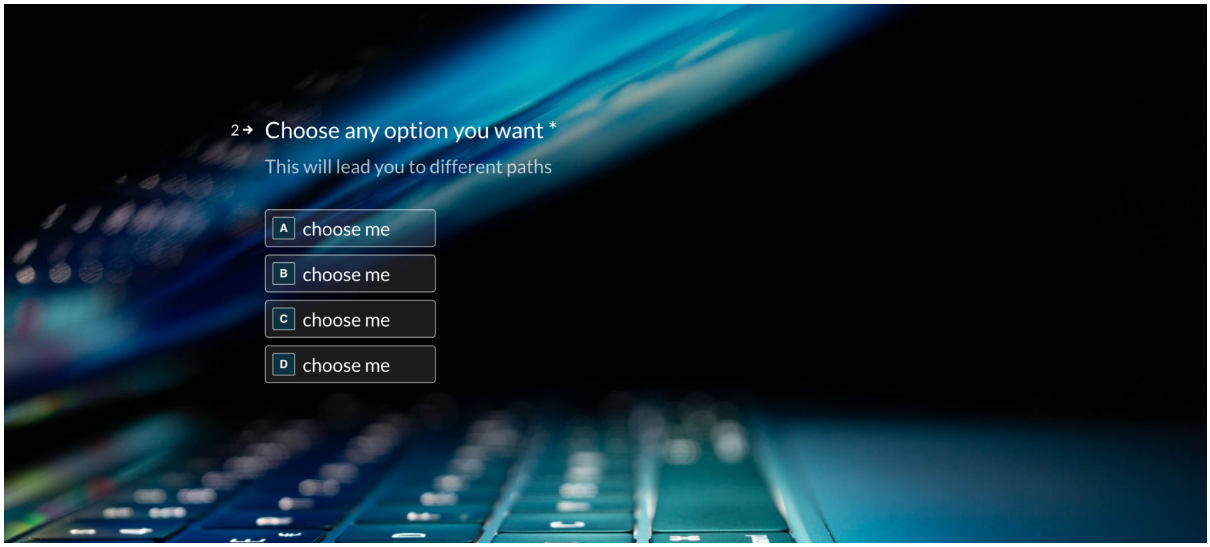
Appendix A

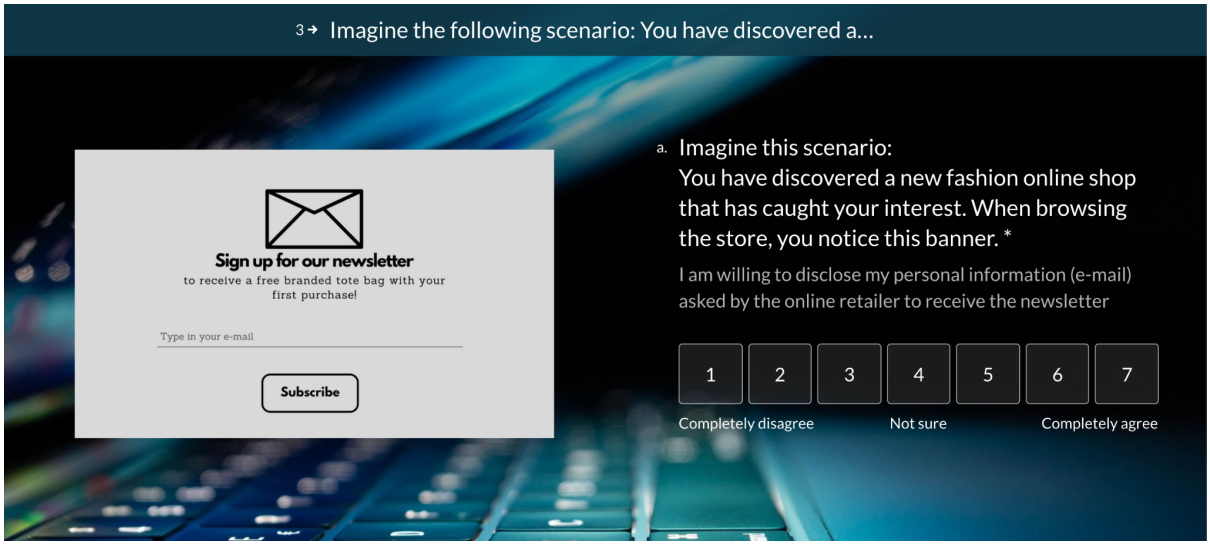
Screenshots of the survey interface

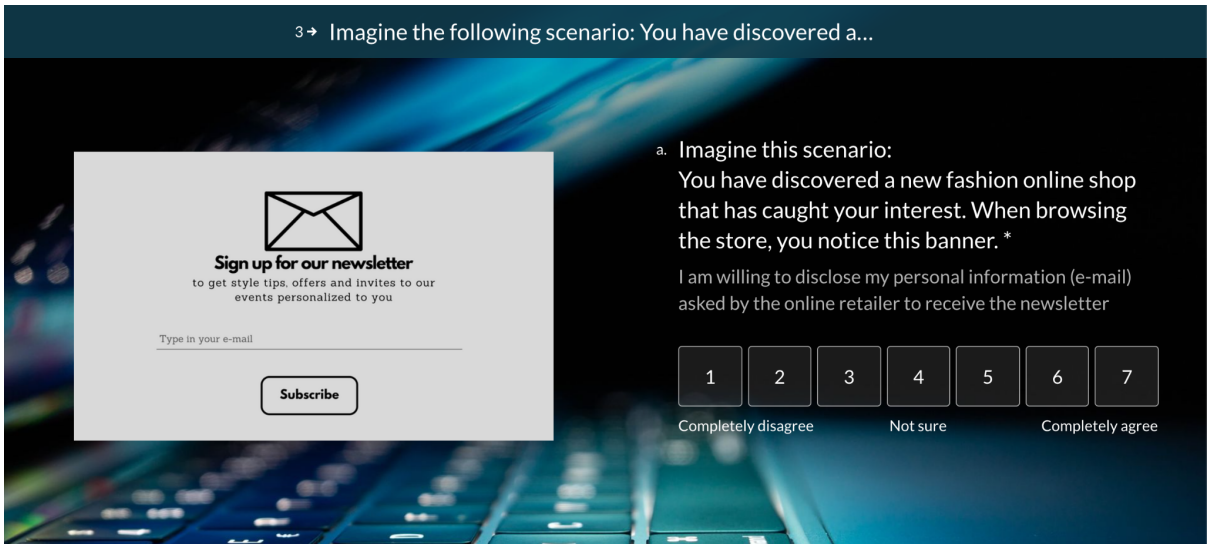
Link to the survey results: https://docs.google.com/spreadsheets/d/1AH-rmDNX5UEYBJLGpeBWtLw5uq03lg1I-ipMMKt4lTA/edit?usp=sharing

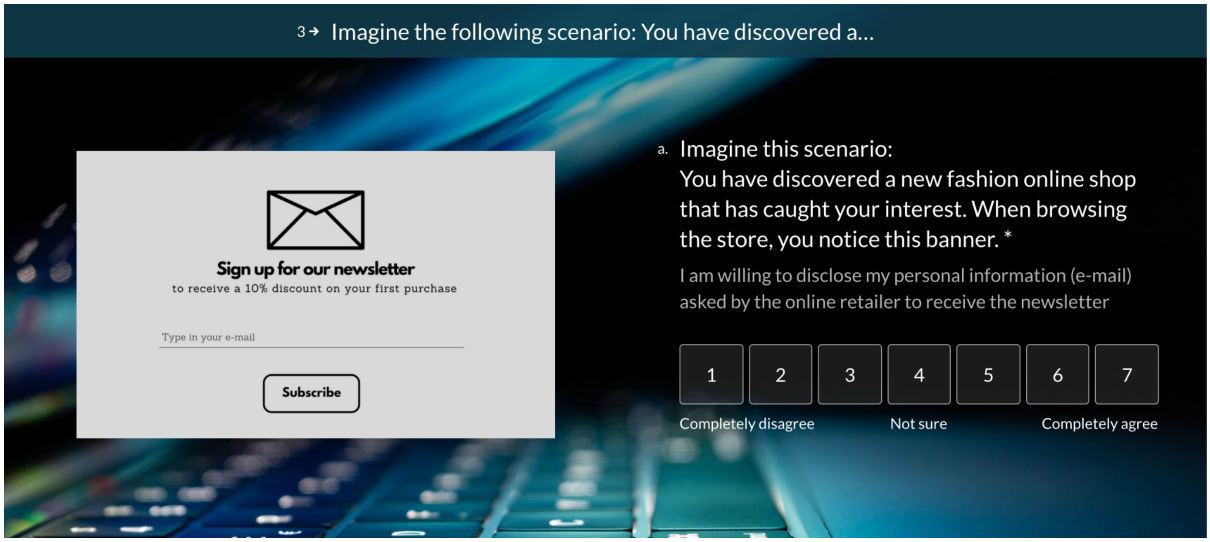


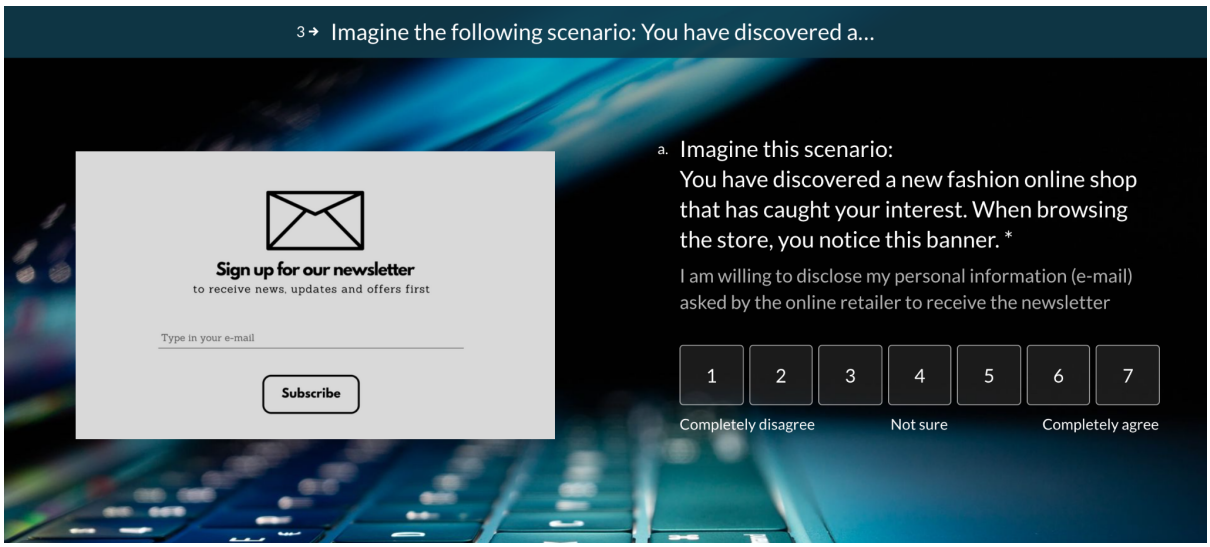


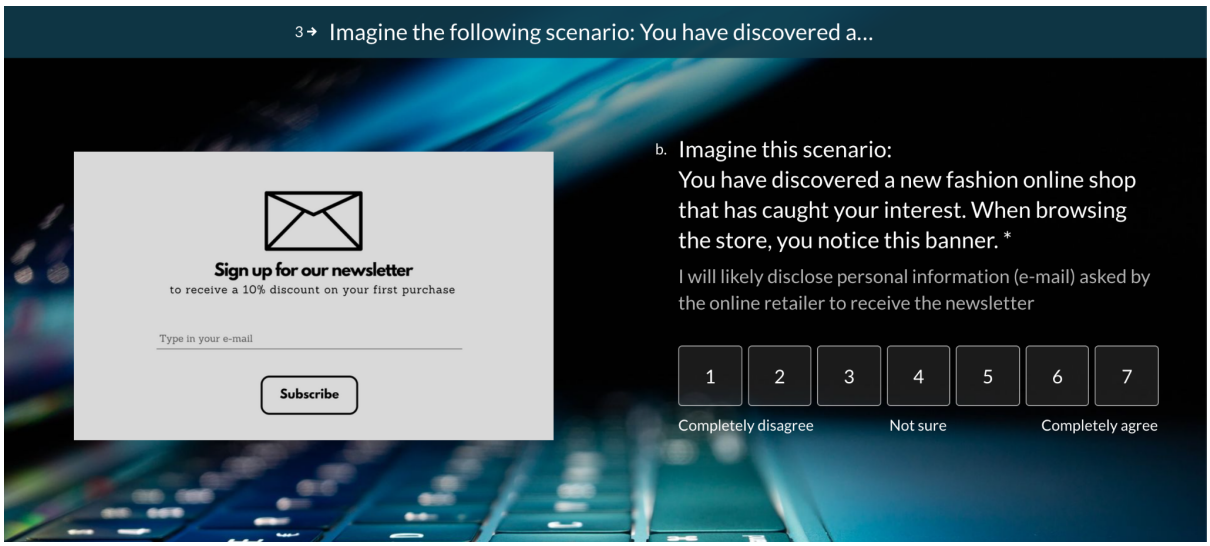

2 → Choose any option you want *
This will lead you to different paths
A choose me
B choose me
C choose me
D choose me

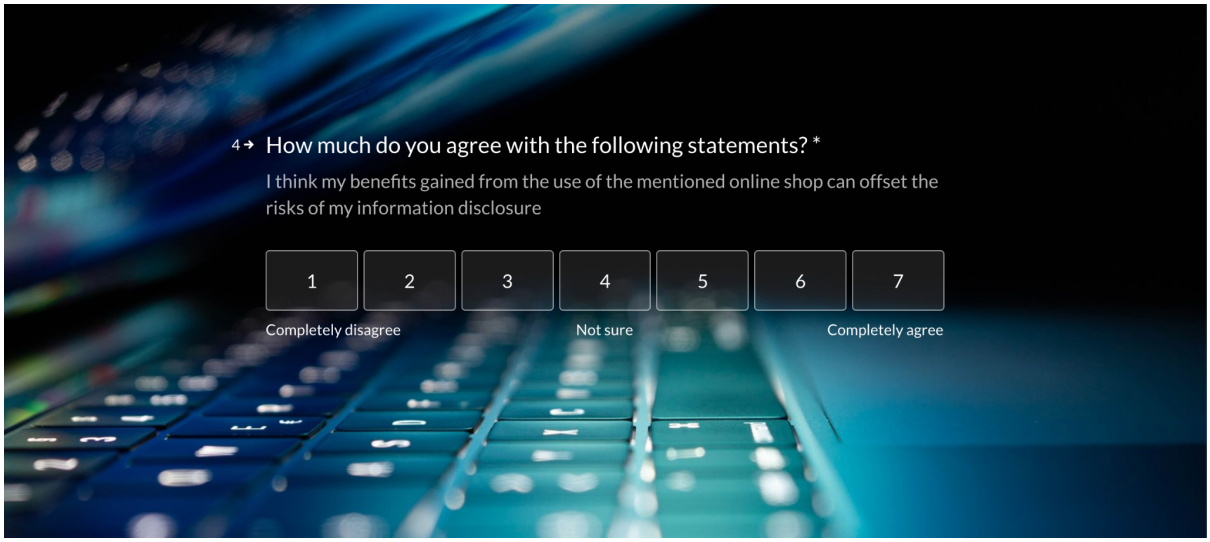

3 → Imagine the following scenario: You have discovered a...
Sign up for our newsletter
to receive a free branded tote bag with your first purchase!
Type in your e-mail
Subscribe
a. Imagine this scenario:
You have discovered a new fashion online shop that has caught your interest. When browsing the store, you notice this banner. *
I am willing to disclose my personal information (e-mail) asked by the online retailer to receive the newsletter
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

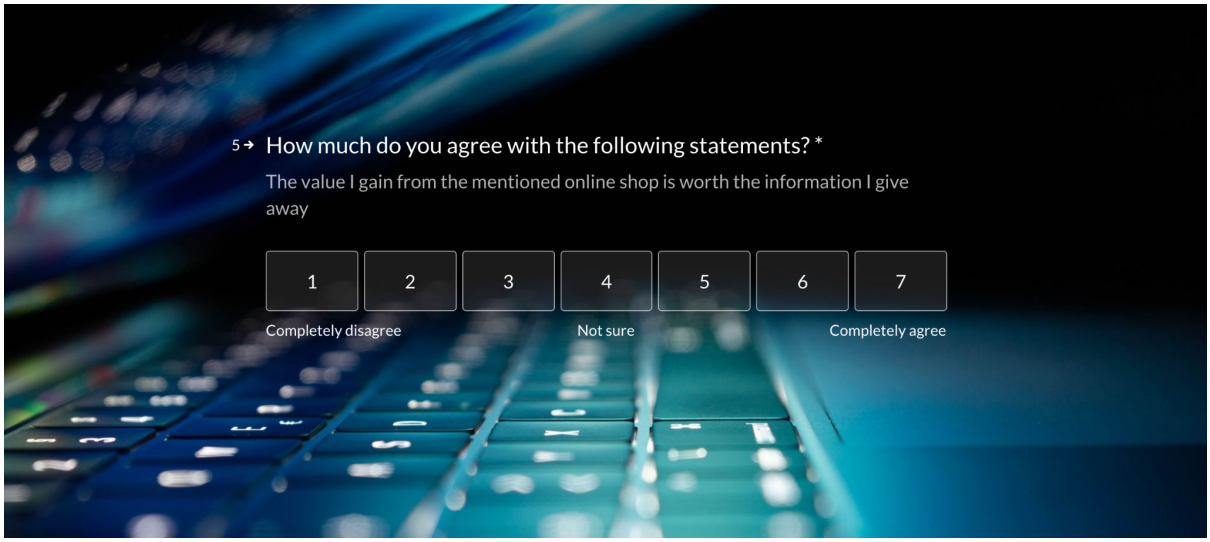

3 → Imagine the following scenario: You have discovered a...
Sign up for our newsletter
to get style tips, offers and invites to our events personalized to you
Type in your e-mail
Subscribe
a. Imagine this scenario:
You have discovered a new fashion online shop that has caught your interest. When browsing the store, you notice this banner. *
I am willing to disclose my personal information (e-mail) asked by the online retailer to receive the newsletter
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

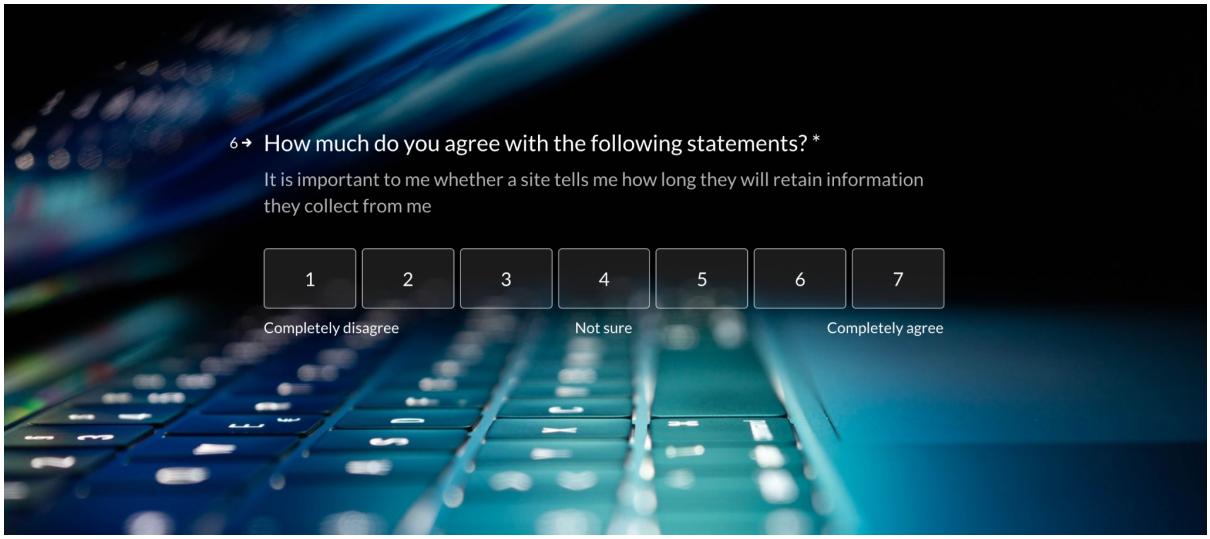

3 → Imagine the following scenario: You have discovered a...
Sign up for our newsletter
to receive a 10% discount on your first purchase
Type in your e-mail
Subscribe
a. Imagine this scenario:
You have discovered a new fashion online shop that has caught your interest. When browsing the store, you notice this banner. *
I am willing to disclose my personal information (e-mail) asked by the online retailer to receive the newsletter
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

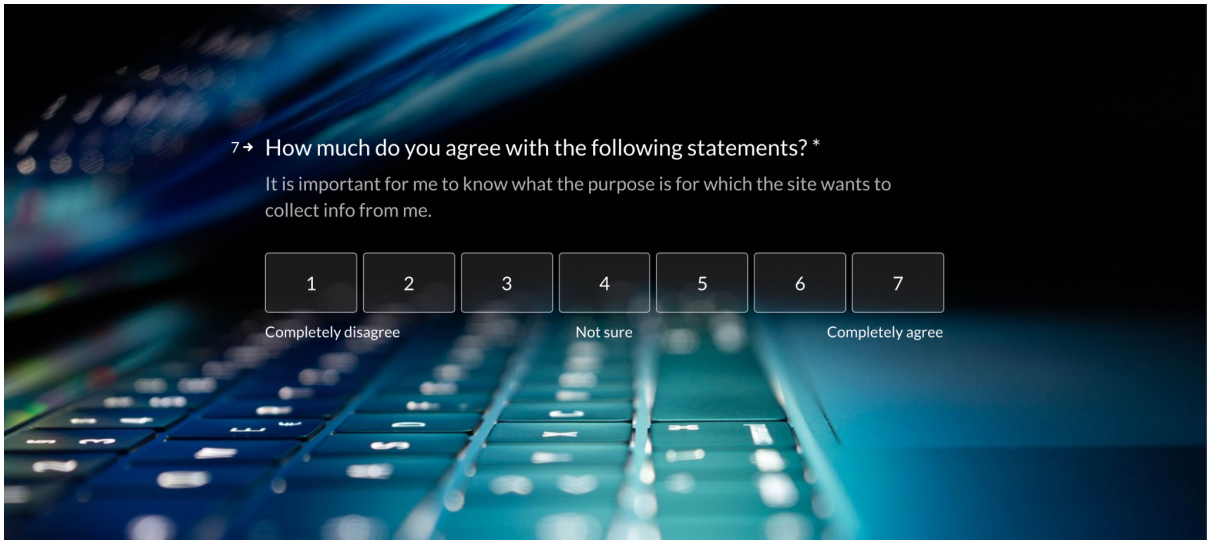

3 → Imagine the following scenario: You have discovered a...
Sign up for our newsletter
to receive news, updates and offers first
Type in your e-mail
Subscribe
a. Imagine this scenario:
You have discovered a new fashion online shop that has caught your interest. When browsing the store, you notice this banner. *
I am willing to disclose my personal information (e-mail) asked by the online retailer to receive the newsletter
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

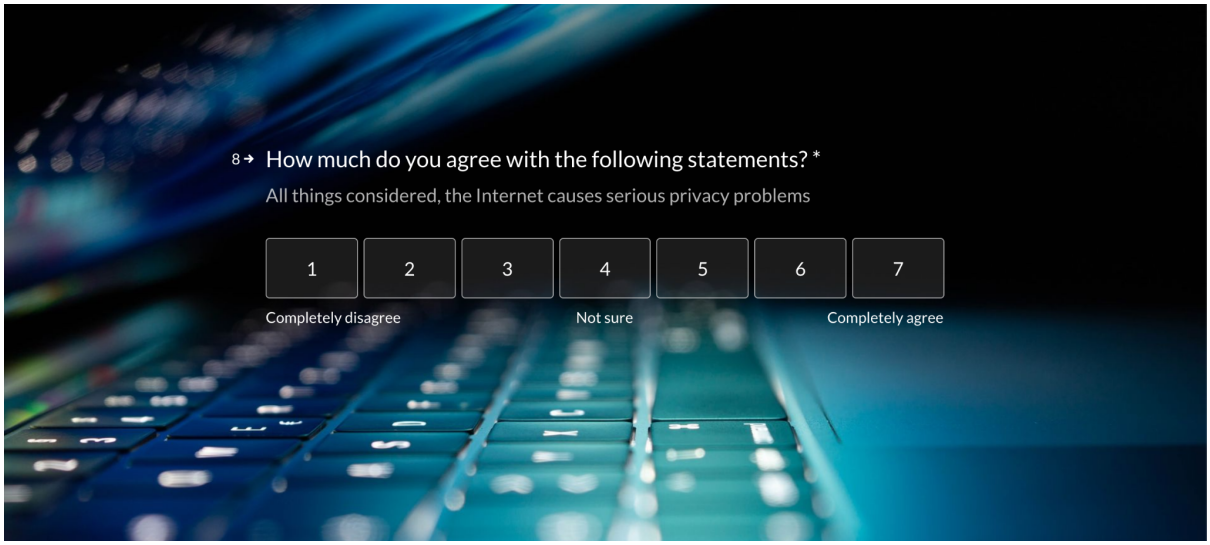

3 → Imagine the following scenario: You have discovered a...
Sign up for our newsletter
to receive a 10% discount on your first purchase
Type in your e-mail
Subscribe
b. Imagine this scenario:
You have discovered a new fashion online shop that has caught your interest. When browsing the store, you notice this banner. *
I will likely disclose personal information (e-mail) asked by the online retailer to receive the newsletter
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

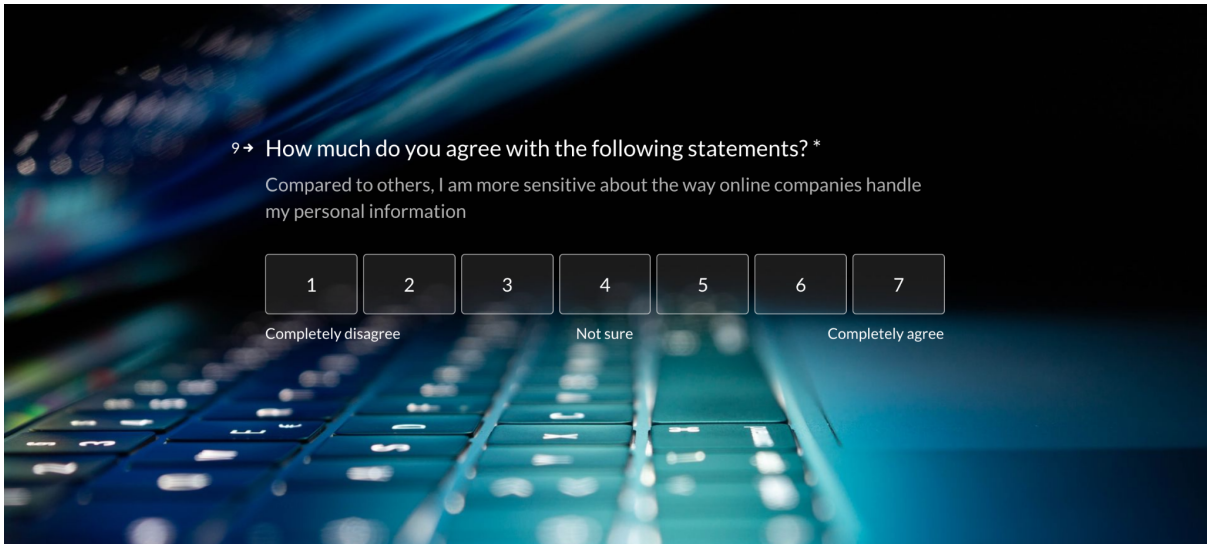

4 → How much do you agree with the following statements? *
I think my benefits gained from the use of the mentioned online shop can offset the risks of my information disclosure
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

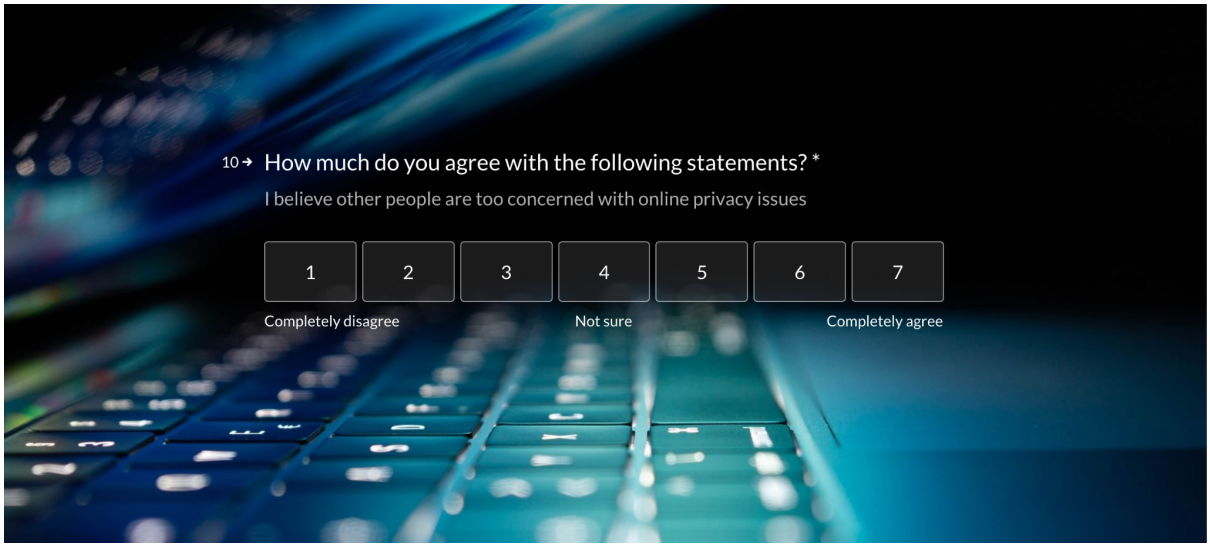

5 → How much do you agree with the following statements? *
The value I gain from the mentioned online shop is worth the information I give away
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

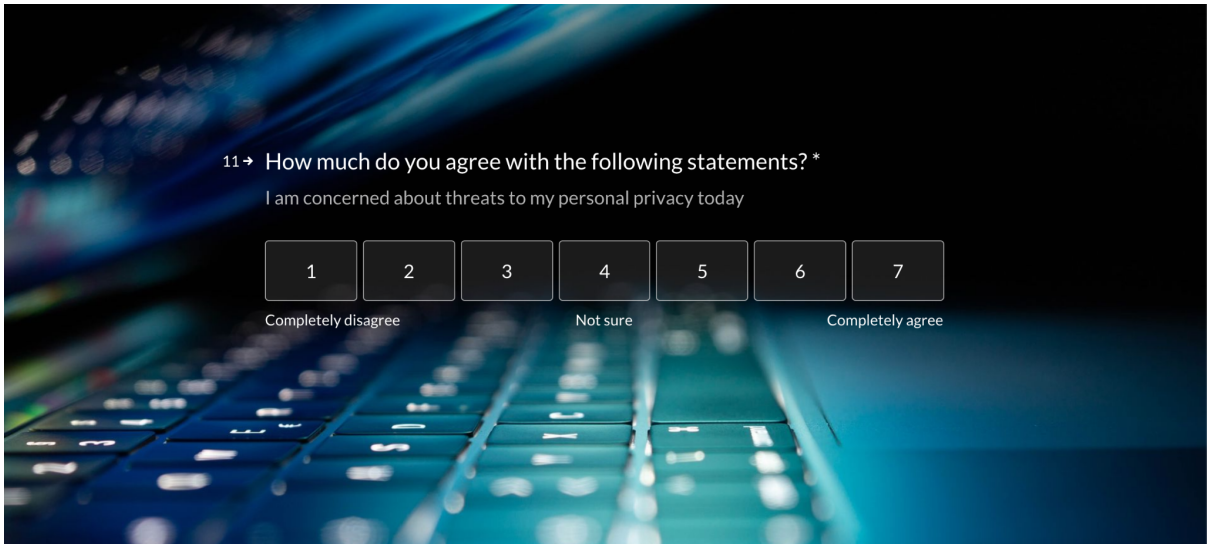

6 → How much do you agree with the following statements? *
It is important to me whether a site tells me how long they will retain information they collect from me
1 2 3 4 5 6 7
Completely disagree
Not sure
Completely agree

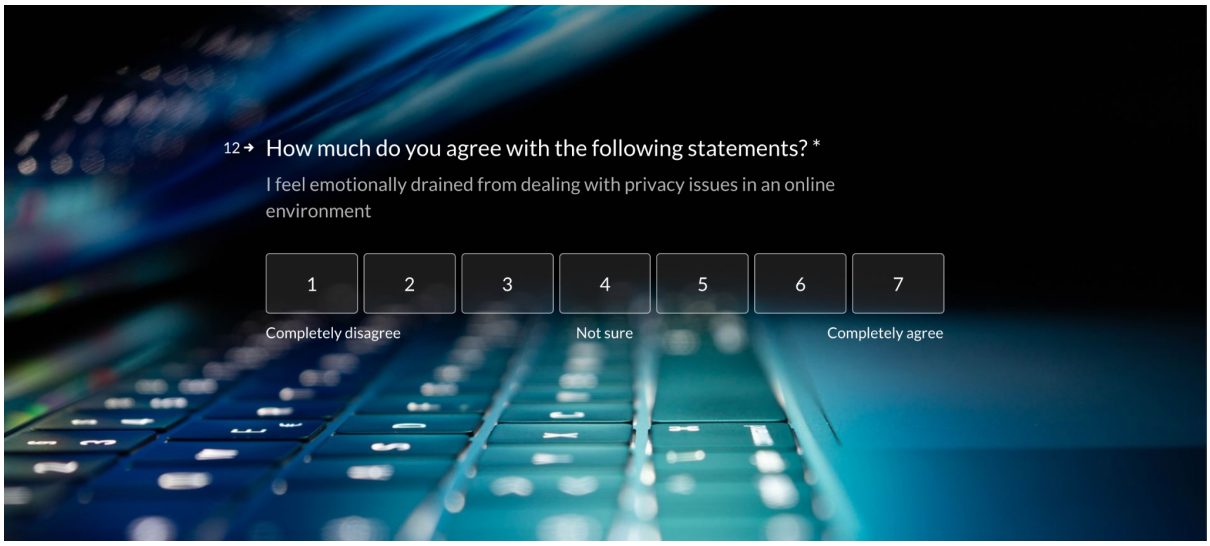

7 → How much do you agree with the following statements? *
It is important for me to know what the purpose is for which the site wants to collect info from me.
1
2
3
4
5
6
7
Completely disagree
Not sure
Completely agree

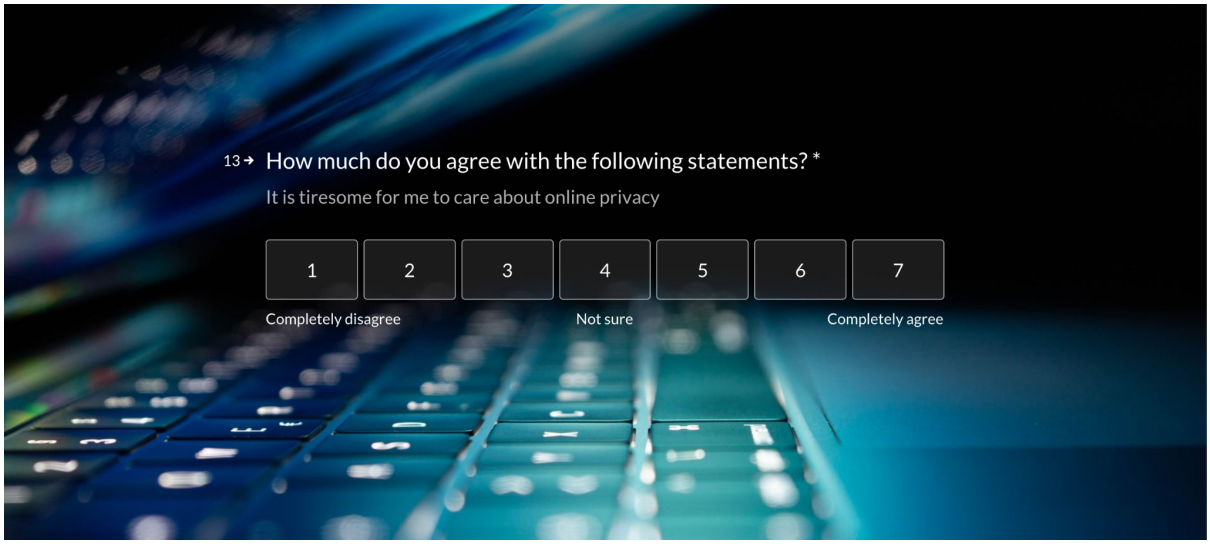

8 → How much do you agree with the following statements? *
All things considered, the Internet causes serious privacy problems
1
2
3
4
5
6
7
Completely disagree
Not sure
Completely agree

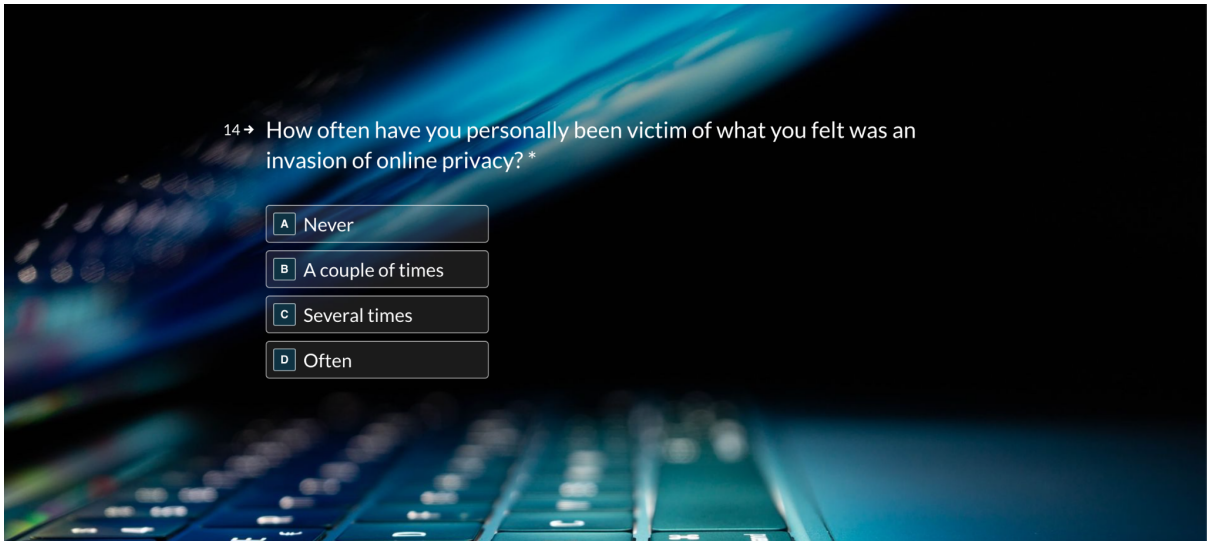

9 → How much do you agree with the following statements? *
Compared to others, I am more sensitive about the way online companies handle my personal information
1
2
3
4
5
6
7
Completely disagree
Not sure
Completely agree

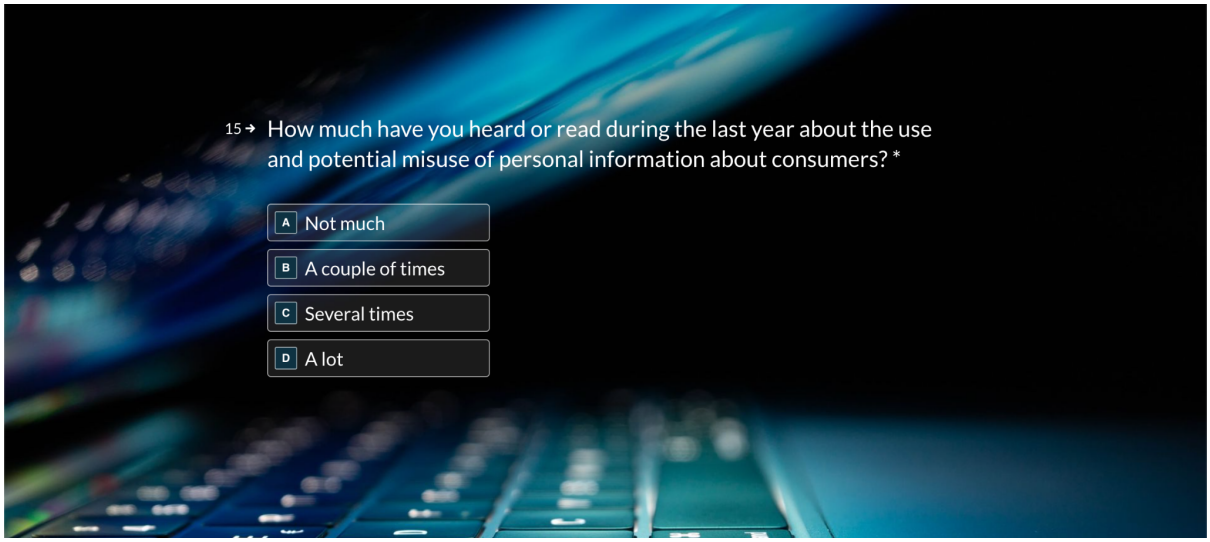

10 How much do you agree with the following statements? *
I believe other people are too concerned with online privacy issues
1
2
3
4
5
6
7
Completely disagree
Not sure
Completely agree

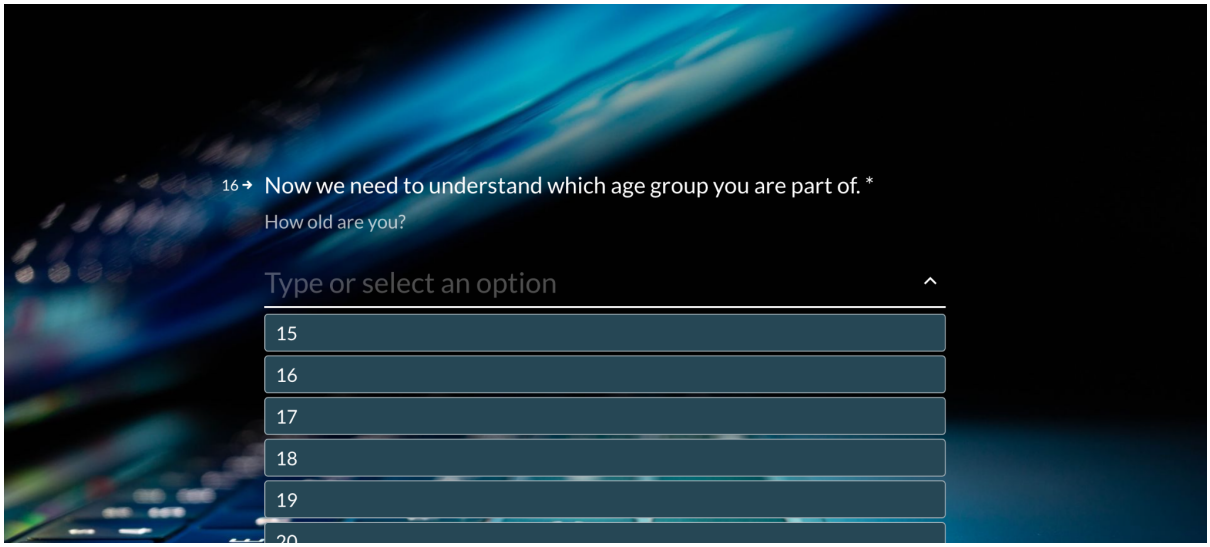

11 How much do you agree with the following statements? *
I am concerned about threats to my personal privacy today
1
2
3
4
5
6
7
Completely disagree
Not sure
Completely agree

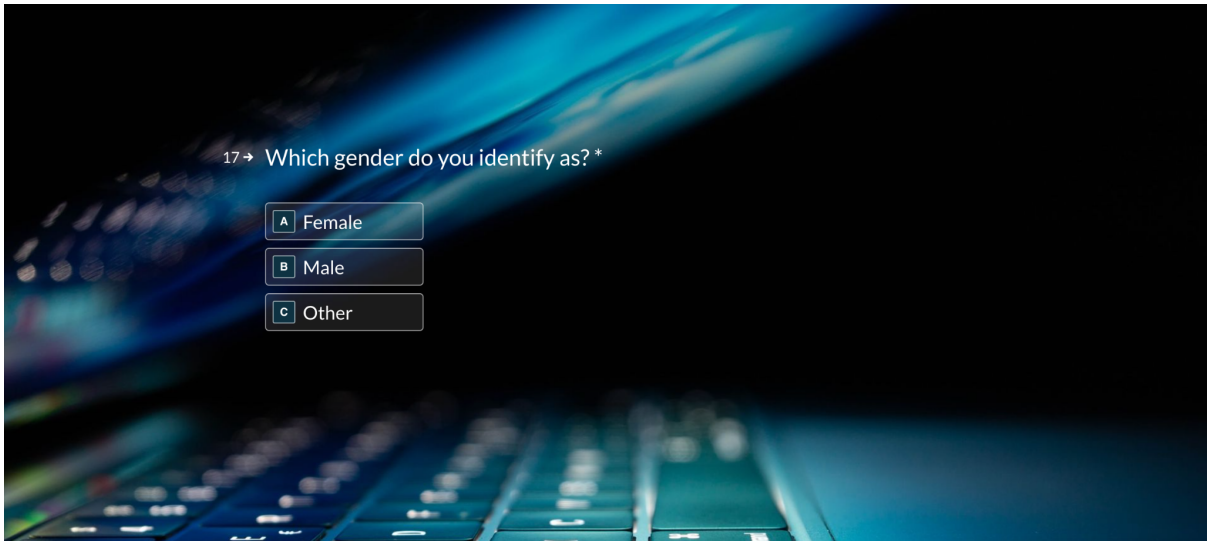

12 How much do you agree with the following statements? *
I feel emotionally drained from dealing with privacy issues in an online environment
1
2
3
4
5
6
7
Completely disagree
Not sure
Completely agree

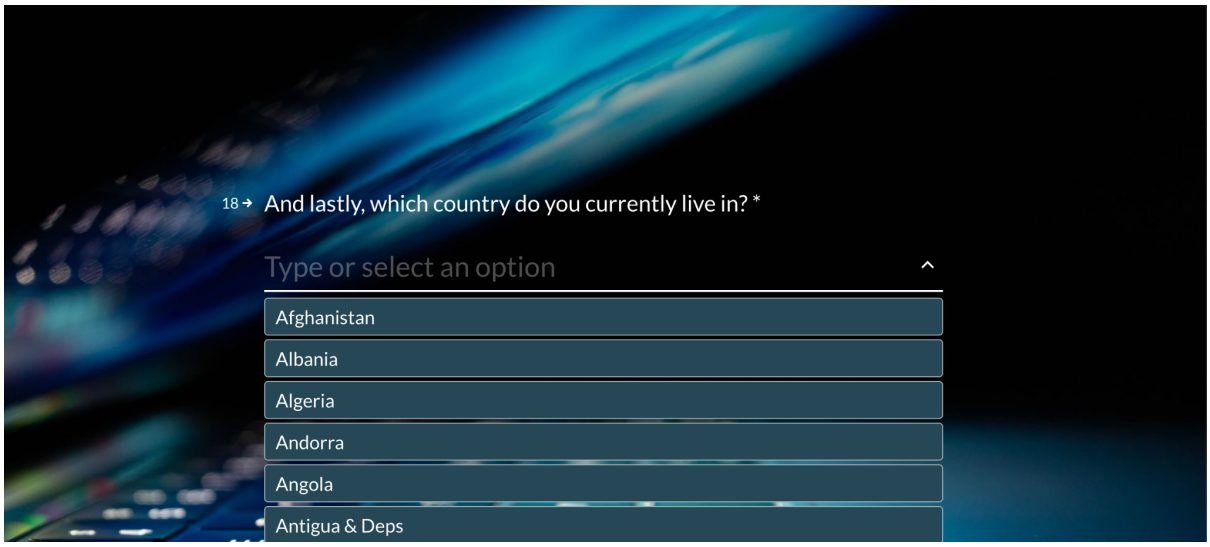

13 → How much do you agree with the following statements? *
It is tiresome for me to care about online privacy
1
2
3
4
5
6
7
Completely disagree
Not sure
Completely agree


14 → How often have you personally been victim of what you felt was an invasion of online privacy? *
A Never
B A couple of times
C Several times
D Often


15 → How much have you heard or read during the last year about the use and potential misuse of personal information about consumers? *
A Not much
B A couple of times
C Several times
D A lot


16 → Now we need to understand which age group you are part of. *
How old are you?
Type or select an option
15
16
17
18
19


17 → Which gender do you identify as? *
A Female
B Male
C Other


18 → And lastly, which country do you currently live in? *
Type or select an option
Afghanistan
Albania
Algeria
Andorra
Angola
Antigua & Deps

Appendix B

Example of an interview guide

1. What do you believe are the biggest challenges for digital marketers right now and how will it affect the industry?
2. What do you think will be the biggest change for your work in 5-10 years?
3. We have noticed many privacy-first solutions emerging right now. New tracking-free browsers, differential privacy, FLoC technology, to mention a few. What do you believe could become an industry standard?
4. Do you believe these differential privacy techniques (as the FLoC technology) will be beneficial for the users and will they even notice a difference?
5. Do you believe that some of the biggest tech giants are capitalizing on user privacy?
6. We conducted an experiment where respondents were asked to share their e-mail with a fictional online shop and get personalization benefits in return. The result was that we actually found it to have a negative effect on their willingness to share their information. Why do you think that is?
7. We also found that even though our respondents were concerned with their privacy, they were still willing to share their data if the value they gained in return was sufficient. Personalization benefits were not enough, as earlier mentioned. In your opinion, what value should an online shop offer users in return of sharing their personal data?
8. How do you advise clients on earning the customer's trust?
9. What role do you think first party data will play for businesses in the future?
10. We often come across websites that do not comply with GDPR, e.g. non-compliant cookie banners. Why do you think that many businesses are struggling to keep up with GDPR-compliance even after a couple of years?
11. Finally, what is your advice for businesses trying to adapt to these privacy-first standards?

Appendix C

Pearson correlation

	Intention to disclose personal information	Hedonic	Personalization	Transparency	Privacy fatigue	Privacy concerns	Value of information disclosure
Pearson Correlation							
Intention to disclose personal information	1	28	-.167*	-54	-39	-130	.608**
Hedonic	28	1	-.354**	50	-40	3	-45
Personalization	-.167*	-.354**	1	-36	-43	63	-112
Transparency	-54	50	-36	1	148	.481**	-104
Privacy fatigue	-39	-40	-43	148	1	.173*	128
Privacy concerns	-130	3	63	.481**	.173*	1	-.172*
Value of information disclosure	.608**	-45	-112	-104	128	-.172*	1
Sig. (2-tailed)							
Intention to disclose personal information		732	41	515	634	113	0
Hedonic	732		0	543	626	973	588
Personalization	41	0		665	598	449	175
Transparency	515	543	665		73	0	205
Privacy fatigue	634	626	598	73		35	121
Privacy concerns	113	973	449	0	35		36
Value of information disclosure	0	588	175	205	121	36	

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

Appendix D

Moderation effects for personalization

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	-.001	.081		-.011	.992		
	Zscore: pers	-.171	.082	-.171	-2.084	.039	.997	1.003
	Zscore(Trnsp_average)	-.060	.082	-.060	-.735	.463	.999	1.001
	interaction_pers_Trnsp	-.024	.083	-.024	-.293	.770	.998	1.002

a. Dependent Variable: Zscore(IDP_average)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	.001	.081		.010	.992		
	Zscore: pers	-.166	.081	-.166	-2.052	.042	1.000	1.000
	Zscore(PFtg_II)	.003	.082	.003	.033	.974	.977	1.023
	interaction_pers_PftgII	.148	.090	.135	1.649	.101	.977	1.023

a. Dependent Variable: Zscore(IDP_average)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	-.001	.081		-.014	.989		
	Zscore: pers	-.161	.082	-.161	-1.974	.050	.989	1.011
	Zscore(PCnc_average)	-.118	.082	-.118	-1.444	.151	.981	1.019
	interaction_pers_PCnc	.018	.088	.017	.202	.840	.979	1.021

a. Dependent Variable: Zscore(IDP_average)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	.000	.066		-.006	.995		
	Zscore: pers	-.101	.066	-.101	-1.527	.129	.974	1.027
	Zscore(VID_average)	.597	.066	.597	9.047	.000	.983	1.018
	interaction_pers_VID	-.003	.064	-.004	-.055	.956	.979	1.021

a. Dependent Variable: Zscore(IDP_average)

Appendix E

Mediation effects for personalization

```
OUTCOME VARIABLE:
 VID_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .1116      .0125     2.6441     1.8544     1.0000   147.0000      .1754

Model
              coeff         se          t          p       LLCI       ULCI
constant     3.8929      .1536    25.3359      .0000     3.5892     4.1965
pers         -.4199      .3083    -1.3618      .1754    -1.0292      .1895

**************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .6162      .3797     2.5088    44.6784     2.0000   146.0000      .0000

Model
              coeff         se          t          p       LLCI       ULCI
constant      .5476      .3467     1.5794      .1164     -.1376     1.2329
pers         -.4643      .3022    -1.5364      .1266    -1.0617      .1330
VID_avg       .7309      .0803     9.0974      .0000      .5721      .8897

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
     -.4643      .3022    -1.5364      .1266    -1.0617      .1330

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
VID_avg     -.3069      .2450     -.7764      .1560
```

```
OUTCOME VARIABLE:
 PCnc_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0625      .0039     1.6526      .5773     1.0000   147.0000      .4486

Model
             coeff         se          t          p       LLCI       ULCI
constant    4.8080      .1215    39.5814      .0000     4.5680     5.0481
pers         .1852      .2438      .7598      .4486     -.2965      .6669

************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .2061      .0425     3.8725     3.2373     2.0000   146.0000      .0421

Model
             coeff         se          t          p       LLCI       ULCI
constant    4.2938      .6349     6.7632      .0000     3.0391     5.5486
pers        -.7365      .3739    -1.9700      .0507    -1.4754      .0024
PCnc_avg    -.1874      .1263    -1.4842      .1399     -.4369      .0621

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
     -.7365      .3739    -1.9700      .0507    -1.4754      .0024

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
PCnc_avg    -.0347      .0585     -.1865      .0550
```

```
OUTCOME VARIABLE:
 PFtg_II

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0056      .0000     3.0696      .0046     1.0000   147.0000      .9462

Model
             coeff         se          t          p       LLCI       ULCI
constant    4.5089      .1656    27.2358      .0000     4.1818     4.8361
pers        -.0224      .3322     -.0676      .9462     -.6790      .6341

**************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .1683      .0283     3.9297     2.1281     2.0000   146.0000      .1227

Model
             coeff         se          t          p       LLCI       ULCI
constant    3.4836      .4606     7.5634      .0000     2.5733     4.3939
pers        -.7717      .3759    -2.0529      .0419    -1.5146     -.0288
PFtg_II     -.0201      .0933     -.2157      .8295     -.2046      .1643

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
     -.7717      .3759    -2.0529      .0419    -1.5146     -.0288

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
PFtg_II      .0005      .0290     -.0557      .0672
```

```
OUTCOME VARIABLE:
 Trnp_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0357      .0013     2.6590      .1880     1.0000   147.0000      .6653

Model
              coeff         se          t          p       LLCI       ULCI
constant     5.1205      .1541    33.2330      .0000     4.8160     5.4250
pers         -.1340      .3092     -.4335      .6653     -.7451      .4770

**************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .1778      .0316     3.9165     2.3818     2.0000   146.0000      .0960

Model
              coeff         se          t          p       LLCI       ULCI
constant     3.7694      .5456     6.9086      .0000     2.6911     4.8477
pers         -.7811      .3755    -2.0802      .0393    -1.5232     -.0390
Trnp_avg     -.0735      .1001     -.7346      .4637     -.2714      .1243

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
     -.7811      .3755    -2.0802      .0393    -1.5232     -.0390

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
Trnp_avg      .0099      .0432     -.0613      .1256
```

Appendix F

Moderation effects for hedonic value offering

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	.002	.083		.021	.983		
	Zscore: hed	.033	.083	.033	.396	.693	.995	1.005
	Zscore(Trnsp_average)	-.056	.083	-.056	-.672	.503	.997	1.003
	interaction_hed_Trnsp	-.035	.084	-.035	-.422	.674	.997	1.003

a. Dependent Variable: Zscore(IDP_average)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	-.010	.081		-.120	.905		
	Zscore: hed	.018	.081	.018	.226	.822	.996	1.004
	Zscore(PFtg_II)	-.002	.081	-.002	-.021	.983	.993	1.007
	interaction_hed_PftgII	-.201	.079	-.207	-2.540	.012	.993	1.007

a. Dependent Variable: Zscore(IDP_average)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	5.349E-5	.082		.001	.999		
	Zscore: hed	.029	.082	.029	.349	.728	1.000	1.000
	Zscore(PCnc_average)	-.130	.082	-.130	-1.583	.115	1.000	1.000
	interaction_hed_PCnc	-.020	.082	-.020	-.238	.812	1.000	1.000

a. Dependent Variable: Zscore(IDP_average)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	.001	.066		.008	.994		
	Zscore: hed	.056	.066	.056	.851	.396	.996	1.004
	Zscore(VID_average)	.610	.066	.610	9.262	.000	.997	1.003
	interaction_hed_VID	.012	.065	.012	.182	.856	.997	1.003

a. Dependent Variable: Zscore(IDP_average)

Appendix G

Mediation effects for hedonic value offering

```
OUTCOME VARIABLE:
 Trnp_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0503      .0025     2.6556      .3726     1.0000   147.0000      .5425

Model
              coeff         se          t          p       LLCI       ULCI
constant     5.0370      .1568    32.1221      .0000     4.7271     5.3469
hed           .1825      .2989      .6104      .5425     -.4083      .7732

************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0621      .0039     4.0286      .2827     2.0000   146.0000      .7542

Model
              coeff         se          t          p       LLCI       ULCI
constant     3.5093      .5469     6.4162      .0000     2.4283     4.5902
hed           .1384      .3687      .3755      .7078     -.5902      .8670
Trnp_avg     -.0680      .1016     -.6695      .5042     -.2688      .1328

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
      .1384      .3687      .3755      .7078     -.5902      .8670

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
Trnp_avg     -.0124      .0363     -.1025      .0485
```

```
OUTCOME VARIABLE:
 PCnc_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0028      .0000     1.6591      .0011     1.0000   147.0000      .9734

Model
              coeff         se          t          p       LLCI       ULCI
constant     4.8519      .1239    39.1458      .0000     4.6069     5.0968
hed           .0079      .2363      .0335      .9734     -.4590      .4748

************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .1335      .0178     3.9721     1.3254     2.0000   146.0000      .2689

Model
              coeff         se          t          p       LLCI       ULCI
constant     4.1519      .6482     6.4052      .0000     2.8708     5.4330
hed           .1276      .3656      .3491      .7275     -.5949      .8502
PCnc_avg     -.2031      .1276    -1.5912      .1137     -.4553      .0492

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
      .1276      .3656      .3491      .7275     -.5949      .8502

Indirect effect(s) of X on Y:
             Effect     BootSE   BootLLCI   BootULCI
PCnc_avg     -.0016      .0557     -.1257      .1209
```

```
OUTCOME VARIABLE:
 VID_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0447      .0020     2.6721      .2940     1.0000   147.0000      .5885

Model
             coeff         se          t          p       LLCI       ULCI
constant    3.8333      .1573    24.3702      .0000     3.5225     4.1442
hed         -.1626      .2999     -.5423      .5885     -.7552      .4300

**************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .6105      .3727     2.5369    43.3745     2.0000   146.0000      .0000

Model
             coeff         se          t          p       LLCI       ULCI
constant     .3005      .3441      .8733      .3840     -.3796      .9805
hed          .2476      .2925      .8466      .3986     -.3304      .8256
VID_avg      .7477      .0804     9.3039      .0000      .5889      .9065


****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
      .2476      .2925      .8466      .3986     -.3304      .8256

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
VID_avg     -.1216      .2339     -.5708      .3426
```

```
OUTCOME VARIABLE:
 PFtg_II

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0487      .0024     3.0624      .3492     1.0000   147.0000      .5555

Model
             coeff         se          t          p       LLCI       ULCI
constant    4.5556      .1684    27.0532      .0000     4.2228     4.8883
hed         -.1897      .3210     -.5909      .5555     -.8241      .4447

**************************************************************************
OUTCOME VARIABLE:
 IDP_avg

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .0321      .0010     4.0401      .0755     2.0000   146.0000      .9273

Model
             coeff         se          t          p       LLCI       ULCI
constant    3.2465      .4729     6.8648      .0000     2.3119     4.1812
hed          .1227      .3691      .3324      .7401     -.6069      .8523
PFtg_II     -.0175      .0947     -.1850      .8535     -.2048      .1697

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y *****************

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI
      .1227      .3691      .3324      .7401     -.6069      .8523

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
PFtg_II      .0033      .0343     -.0781      .0745
```

Appendix H

Interview with Rhys Cater, 2021.04.14

Interviewer 0:01

First of all, we would like to know, what do you believe are the biggest challenges for digital marketers right now? And how will it affect the industry?

Rhys 0:15

Yeah, sure. Well, I suppose to start with one of the biggest challenges I think the digital marketers face in general, is that it's a huge topic that encompasses so many different things. So digital marketers are often juggling many, many different topics, like, you know, the products that they work with are often highly technical and highly detailed. If you think about the work that Precis does in the product, it's near requires a great deal of technical depth and understanding, then, of course, they've got to really have a clear idea of what they're trying to achieve for the business, building strategy and helping to, to understand how digital marketing fits in with the priorities of the company. And then they've got, of course, coordinate their budgets, with other departments with no traditional and offline marketing, understanding the balance, understanding how those things compare. It's a really, really complex job, you often hear thrown about that CMOs have the hardest job in any company. I don't know if that's just people being biased, but you know, I'm prepared to believe it, because their scope is so wide. And, of course, privacy. You know, the topic of today's conversation, I suppose, is, is another area that, you know, previously digital marketers, I suppose, not that they didn't have to think about it, but it certainly wasn't as high on their agenda, as it is today. And suddenly, it's this whole new area that's really big, really complex, you know, suddenly, digital marketers, in addition to being technical experts in channels, strategic experts in business, also have to understand a whole bunch of legislation like the GDPR and cookie laws, legislation that's quite rapidly changing and evolving legislation that hasn't really yet got much precedent in trials and courts. So everyone is in a super kind of gray area with with, like, how the legislation and the guidelines are interpreted. All of that's really complex. And then, of course, you know, translating what that legislation and what the changes in technology regarding privacy, and what changes in consumer expectations

actually mean, for the work that they're doing day to day? That's a huge challenge. So I suppose to put it quite simply, the biggest challenge that digital marketers face today, I think, is that they're expected to do far too much stuff. And often they are under resourced, and under prepared to get that they don't have the legal, the technical and data support the senior buy in with companies regarding strategy to get the things done that they do.

Interviewer 2:50
Okay, very interesting. What do you think will be the biggest change for your work in five to ten years?

Rhys 2:56
Yeah, I think that we're already starting to see some of that change. If we look at the short term change, I suppose within the next, you know, kind of five years, we're already starting to see a bit of that. So, you know, I think if you look at the recent past, what companies were basically, buying when they were hiring digital marketing experts, or hiring digital marketing agencies, was technical expertise. You know, if you look at what Precis was doing, we were positioning ourselves in the skills gap a little bit, where we know more about the technical stuff than other people do. And hence we can, we can kind of add value. But that's rapidly changing. You know, nowadays, it's it's pretty simple to find people who who've got those those technical skills or easier that used to be. But also the, you know, the platforms themselves, like Google and Facebook, with a digital marketing, I've just heard that the easier they make their platforms to use, the more accessible they can be, and the more money that Google and Facebook will make, so that they're easier to use as well. So really, the nature of digital marketing is changing away from being something that requires, you know, more technical skill than anything else towards requiring more business creative and strategic skill than other things. So I think the five year change is going to be exactly that. Which is where, you know, where we see a whole lot of uncertainty. This privacy stuff, you know, it's going to drag on for years. So it'll be a lot of a lot of turbulence, a lot of uncertainty. And the skills people will need will be people who can really bring direction to things. Looking further out again, into the 10 year horizon. I wouldn't be surprised if we see a bit of a swing in how things go. You know, I think we're going to go through a five year period now where we can

Use much less data. And privacy, you know, it revolutionizes how we do things and, you know, it starts to limit like the ways of working that we had in the past. And I think it puts the brakes on data usage. But if you look a bit further down the line, I do believe that, that the laws will develop and change and practices and understandings of how they should be used will develop and change. Yeah, there was a, there was a good article that I shared the other day about, which appeared in the, in the Financial Times by one of the, by a politician in the UK, who was writing about sort of the fact that, you know, we see that data brings enormous advantages and allows us to do things faster and more effectively in many cases when it's used correctly. So it's not to say that privacy isn't important. Of course it is. But it shouldn't come at the expense of being able to do great things with data. And I think that it'll take us a few years to figure out how to do that. But once we do, I think we'll see a whole another revolution where suddenly there's all these new ways of doing things that swing back the other way, almost, that would come maybe, you know, a lot more technical again, because we'll have figured out like the kind of way to do this in a in a way that's like society accepted as it were.

Interviewer 6:22
And when you say that laws are changing, do you think it's also not only GDPR? But when we see like different local laws being made, like in Australia, they have their own very privacy concern law. And we see right now also in China, I think there's been some different local ones. Is that the ones you're talking about?

Rhys 6:41
Yeah, I mean, in terms of the laws, yeah, of course, I'm talking about GDPR. I'm talking about all the local, the ccpa, the Australian variations, the Brazilian variations, they're all of these different laws. And that's the stuff that's going to kind of, you know, put the brakes on whatever we're doing with data and force everyone to step back and reflect, I think that's good. But then, you know, after kind of five years time, in the five to 10 year horizon, I think we'll look back on this time and look back on this legislation, and hopefully, it will develop a lot to become more nuanced. Because right now, it you know, I think if you look at stuff like cookie laws, it's a bit silly, you know, the whole kind of thing of like cookie notices on every

single website, like it's a horrible experience, if you think about the experience the users getting, I would argue that makes people's experience worse, not better. It's obviously very well intentioned, it has good results in the sense that it forces people to reflect on, you know, how they using customer data. But from a, from a usability of the web perspective, these laws are pretty bad, I think, in many cases, Cookie notices everywhere. So I think things like that will just become better, where we start to be like, Okay, well, we can use data in these in these ways. And it can be very valuable to use it and, and customers or people as well, as lawmakers, like understand where the limits are, and will end up in a place where like, the web is more usable. Data is also more usable, and we have more of an equilibrium. I think that's that's probably what's in the, like, 10 year horizon.

Interviewer 8:10
And we've noticed many, like privacy first solutions emerging right now. We see new new tracker free browsers, differential privacy, FLOC-technology to mention a few. What do you believe could be an industry standard in the future?

Rhys 8:27
Well, that's, that's the million dollar question. And if you can answer that, then you're laughing. I think, you know, we'll struggle to I think the honest answer is that we might struggle to converge around an industry standard for some time. If you think about the incentives that Google has, versus the incentives that Apple has, you know, I just, I can't imagine them coming together in the short term, and finding a solution that Apple's happy to implement in Safari, and that Google is happy to implement in, in Chrome. So I actually think that we might end up quite some time with a bit of a two speed system, where, you know, people using different browsers do you end up with with differing levels of, you know, like, data usage and kind of capabilities when it comes to, to marketing. I mean, we already have a little bit of this a precedent for this type of thing where, you know, if you download a game today from from an app store, you know, you can choose to have the ad supported version of the game for free. Or you can choose to have a paid for version of the game that doesn't have ads in it. And I do, I do sort of feel like we've been circling around this idea for the web for a really long time. I wonder if in the next 10 years, we'll we'll actually figure that

out Where, where, you know, there's an ad supported were banned. Anonymous. Supported web kind of thing. And I think that's a very interesting thing to explore I, I find it hard to imagine that we're going to converge around one standard for an ad supported web that everyone is happy with.

Interviewer 10:14
Do you believe that these differential privacy solutions as the FLOC-technology will be beneficial for users? Or will they even notice a difference?

Rhys 10:24
I mean, if you look at what floc is, it's basically the same stuff that was always happening, but with a different technical implementation. So this comes down to what we think that users and I guess lawmakers care about, you know, which is Does anyone actually care about the third party cookies? I think the answer is no, no, no, the average user couldn't care less you know, about their cookies, the reason they care, is because of the effect it has on them, you know, the fact the fact that they see, you know, ads that kind of, you know, follow them around the internet, that kind of stuff. You know, that's, that's what, that's what, that's what people care about. And if you look at what FLOC is trying to do, it's trying to enable that same behavior. But by using a different a different set of technologies, you know, it's it's stuff that happens locally in the users browser, rather than bouncing data around on servers. So I don't actually, I'm quite skeptical about FLOC. I think that FLOC is obviously an interesting, technical solution. And I think if what the purpose of if what consumers wanted, and the purpose of lawmakers was to end up exactly as we are today, but without using third party cookies, then it would be a great solution. But that's not really what these laws are about, right? Like, I mean, if you think about what most people care about with privacy, it's who has access to their data, and what is it used for, really, you know, and arguably, you know, floc enables their data to be used for the same purpose as it was before just in a bit of different way. And the end result for that customer is kind of the same. The level of control that floc offers is a bit higher. I think it is a step forward, for example, that in floc, you know, you can turn on or off, in theory, tracking in at the browser level, so that affects all the sites you visit. So, you know, that would reduce the need, for example, for every single website across the

entire internet, to have like cookie notices and stuff like that, you know, it means that users have like a central form of control. But how easy Google makes it opt in and out will be a big a big thing of like, how much users wanted that technology, I feel like, and I guess, ultimately, like, what's kind of interesting about the browser technologies is that, you know, what you often see is that you, you see browsers being described as a user agent, that's like another term that gets used to describe browsers. And well, that's really what it is, right? Like, the browser is supposed to be your agent, like acting on your behalf, like, you know, my browser, a lot being installed on my computer, there's a big school of thought that that browser should always be acting in my best interests, you know, in the same way that I would not expect my browser to allow, very simply allow people to, like, hack my computer, for example. You know, it's reasonable to also assume that, I would, I would understand that my browser doesn't like, you know, use my personal data in ways that I don't, I don't agree with and can't and can't control. So, that's, I think the interesting debate about things like floc is that, you know, it is it is solving a problem. But I think it might be solving the wrong problem.

Interviewer 13:57

Okay. We also conducted an experiment where respondents were asked to share the email with a fictional online shop. So we asked them to share the email and in return, they would get personalization benefits. And the result was that we actually found it to have a negative effect on their willingness to share the information. Why do you think that is?

Rhys 14:21

Yeah, it's interesting. I think the level of trust that customers have is is super low. You know, if you look at the average person's you know, if you talk to a friend who doesn't work in our industry, or or parent or whatever, like they, they are likely to treat digital marketing and the internet, especially with regards to this data stuff with with quite a lot of mistrust. I'm interested to hear that about the research just because, you know, I think there is a big school of thought that sort of argues that you should give customers an incentive to share their data. You know, so that they understand, because I think one of the fundamental problems with with privacy is that there's a kind of deal that's been made on the internet that nobody ever,

like, agreed to, which is you get to use Google Maps, Instagram, whatever, for free. And in exchange, you know, we use a lot of your, your data to, to kind of, you know, to show you adverts that are more relevant, more measurable, and that's, you know, benefits those companies that are those ad vendors. And I think, you know, the fact that people don't feel like they get that much back from that exchange is like one of the problems so then, you know, and you say, Well, if you give us your email, you get these, these benefits, that people might be more open to it. But I don't know why people would would would, you know, would decline that, I guess it depends a lot how you position it, and how you present it to them how you word it, you know, that lack of trust, you know, it might be the fact that people think, Oh, well, this is too good to be true kind of thing, almost, you know, like, I can't believe that you're going to give me this like 10% off or whatever, just for giving you my my email, like, what's the catch? Like, you know, that's just a thought, I don't know.

Interviewer 16:17
Like, a hidden trade off. They're not really sure what they're giving exactly, maybe. Hmm. Okay. We also found that even though our respondents were concerned with the privacy, they were still willing to share that data if the value they gained in return was sufficient. So like you mentioned, at discount of 10%, or something similar. So personalization benefits were not enough, as earlier mentioned, but in your opinion, what value should an online shop offer us a return of sharing the personal data?

Rhys 16:46
Hmm. I mean, it's a really, it's a hard one to answer. I mean, the the true answer to that. One is that you'd need to probably test it right, you probably need to present various different offers it, it also depends entirely on the business, right? Like, I mean, it's going to be different, a different question, if you're buying a 250 pound dress versus 15 pound, like DVD, not that anyone buys DVDs. But, you know, like, you know, it would be I guess that kind of incentives and the models would be, would be very different. I also feel that people are, you know, more likely to, to share their data with, with brands that they trust and have a longer term relationship with, where the benefits are kind of clearer. You know, if I, and this is like, totally anecdotal, but if I buy, you know, once from a shop, I'll do the guest Checkout, you

know, but if I'm buying regularly from something, you know, I kind of want them to remember my address, and like, stuff like that. So I'm much more likely to give them a give them more of my data and make an account and whatever, whatever, whatever. So, you know, I think it's a little bit more simple than like, just a monetary exchange, right? Like people value convenience, people value trust, you know, that kind of stuff. And so I think that if you do reduce it to like a monetary exchange, like, you know, I could definitely see how that might, you know, come across as a bit kind of crass in a way. You know, like, we're just gonna, like, pay you for your email, like, you don't really get like more benefits than that. You know, you mentioned personalization. I think people don't understand. Super Well, I think if you say to people, like, give us your data so that we can give you more relevant stuff. I think people just expect relevance of the internet nowadays. So it doesn't always like work? Well, you know, I think I think like convenience and stuff like that is like a much more, potentially a much more powerful tool.

Interviewer 18:55
Cool. And speaking of first party data, what role do you think this first party data will play for businesses in the future?

Rhys 19:04
Yeah, well, that this, this actually touches on a really interesting question as well, that I often think about with this topic, you know, people often talk about my data, you know, I think but my data, like when I browse a website, and there are cookies, or I enter my email address, you know, that's like, my, my data. But yeah, to a degree, it's, it's not only mine, right? Like, it is a little bit the businesses as well, like, you know, who owns who owns that data, like really? Well, you know, I mean, I bought something like the date that business has done something to like, earn that data as well. And I would argue they have some ownership of it, you know, I understand that it pertains to me, it's my email and things like that. But, you know, I think sometimes the narrative goes too far with like, who owns this data, you know, is it like an individual has the right to like fully own all of their data always and forever. Order you know, order as people go around the internet, kind of giving it out like other other other parts. Do you have like some right to ownership over? That is kind of an interesting

question. But your question about the importance of first party data? Yes, obviously, it's super important. But it's, it's not just about, you know, gathering it, it's about gathering it with the right legal basis to actually do something with it. You know, because just having it doesn't mean you can necessarily use it for anything, you know, if I collect your email address, in order to process your order, that doesn't automatically mean, I can use that email address to market to you anymore. So, you know, having having this, this, again, is one of those areas that like, I think we'll see a lot of development about in the next 10 years, because right now, you know, the industry is kind of converged around consent, as being the only legal grounds that's really valid to use some of these data for marketing. And what that means is that, you know, you have all these checkboxes and these like banners and these prompts that ask people to share their data for marketing purposes. I don't know how that will develop, you know, I think there will be a big movement tried to push the like, alternative models for legal grounds, to process data in that way, and to use data for marketing. I feel like you know, this kind of focus on consent or nothing. Again, just coming back to the user experience, like I don't think it's always great, because you've got, you know, lots of checkboxes and lots of questions to have to answer. And it makes the processes like very long and complicated. So.

Interviewer 21:46
And speaking of consent, we often come across websites that do not comply with GDPR also, for example, the non compliant cookie banners. We've also had a discussion around it the Precis, why do you think that many companies are struggling to keep up with GDPR compliance, still, after a couple of years?

Rhys 22:05
Yeah, are they struggling? Or are they just willfully not doing it? I would say that in many cases, it's the latter. I think that it's a combination of things. I think there's a lot of fear and resistance to change your businesses, you know, they've established these ways of working that assume that they can, you know, to use a basic example, trigger analytics on every single page, and to tell them that overnight, they're going to lose 70% of that information, because they have to proactively ask for consent is, is pretty, pretty crazy. For some businesses, kind of contemplate even, you know, three years down the line from GDPR launching. The other

thing is, you know, I think the regulators haven't been that aggressive. Really, I think it's a tough spot for regulators, because I think, you know, it kind of fades into this very interesting thing as well, which is that, you know, the GDPR and, and all that, you know, associated laws, and everything else, that they're hardest to comply with, for smaller companies, usually, who, who can't, don't have the resources to, like properly understand the legal ramifications, you know, don't don't have the technical resources to develop good cookie banners, whatever. And then, you know, companies like Google and Facebook, who I mean, you know, outwardly look like they're trying to comply with the law, but in practice, do things that, you know, they're not really super compliant. And they, you know, they have been fined and things like that, but like, I guess, I'm trying to say is like, the regulators, I think, focusing a lot of time and energy on trying to get Google and Facebook, and those sorts of companies like the big players, to change their practices, they've made laws that affect everyone, but their time and attention is really on those big players. And so, you know, the lack of like, action against normal, normal, you know, mid sized businesses or whatever, you know, complying with like, GDPR. That'd be like a couple of cases. But I think a lot of companies have been slow in in like, adopting their said, you know, right now, like, you've seen the standards are not super high. So, even if you just have a cookie banner in the first place, even if it's not perfectly compliant, you know, you could argue, well, it's better than it's better than nothing. And there were lots of websites like doing worse. So I wonder if, you know, just the slowness of like, the industry overall is part of the year. I mean, yeah, but looking at the, you know, look at the playing field like, it has changed a lot in the last two to two years. If you look at it, like two years ago, there were many sites that had cookie banners, but in practice, were just like, you know, letting cookies fire here everywhere, like you know, before consent was given. If you look now like it has changed There are a lot more websites complying. And we did a study at this in the entertainment vertical recently comparing, you know, January 2019. To now, and it's like, you know, it's a totally different picture of like, how much cookies are triggered before and after consent? It's much, much more compliant now than it was so. Yeah. I mean, these laws are designed to I don't think anyone expected, you know, even the legislators, like no one expected people to be fully compliant overnight. You know, I it's a long process, it's a big brief period of change. And I guess that's also why they haven't been like super aggressive, but like handing down fines and stuff like that, but that time will

probably come. Before we decided, like, you know, let's, let's take some action, like set some examples, and nobody wants to be the example. Right?

Interviewer 25:47
That's true. So we only have this last question, it's a big one. And also allows for reflection. what is your advice for businesses trying to adapt to these privacy-first standards?

Rhys 26:02
So I think, my, my first piece of advice would be, I suppose, you know, kind of take it seriously. And by that, what I mean is, is you're really setting up working groups around it, that cover the whole business, you know, it's not just something that covers digital marketing, like you need people involved from legal, from marketing from BI, you know, from the senior leadership, like, you really need a lot of buy in. Because there is a lot of organizational change, like that's happening with this stuff. So yeah, having a really cross functional senior Working Group on this topic is, is critical. And, you know, with that, you know, I would, I would typically also recommend acting sooner rather than later. And going over and above the minimum requirements. The reason I say that is, first of all, it's pretty clear which way the wind is blowing, you know, like, these laws aren't going to go away in the next years. You know, like, like I said, if you look at five year horizon, it's probably going to get stricter. Whereas, like, maybe if you look at 10 years away, like, you know, things might start changing a little bit, but by that time, it's so far away, it's impossible to plan for. So what you should plan for for now is, is, you know, for privacy to be on the agenda for like, the next few years, pretty highly. And as the business you know, it's not a great look, I think, to be just doing the minimum possible on this area, you know, soon enough customers will expect it from businesses. You know, it will be probably a differentiator when it comes to whether people choose to, to buy or not from a company, like how easy or difficult they make it to control this kind of stuff. So I think it will pay off to be a bit bold in this area. And to and to go over and above and yeah, because it's a because it's an organizational change piece. That's why this like cross functional senior working group to look at it is is so so critical. So yeah, I guess in a nutshell, that would be my advice.

Interviewer 28:11

Okay. Thank you so much for an amazing interview.

Appendix I

Interview with Morten Køhler Hansen, 2021.04.16

Interviewer 0:11

First, I would like to give you just a short introduction on what we're going to do today. So our master thesis project investigates the future of digital marketing, as Amanda mentioned. And we would like to ask you some questions regarding what you consider to be best practices and how you as a manager are navigating in these ever changing digital marketing times and digital marketing landscape. And I just wanted to emphasize that this interview will be divided into two parts. So first, we will talk about privacy policy and technology. And then we'll ask for your opinion on some findings that we've already gathered in our research. We're good to start, right. So first of all, what would you say are the biggest challenges in the current digital marketing environment for you as a manager?

Morten 1:02

Well, right now, it's about adjusting to a cookieless future. That is one of the biggest challenges. All of the big platforms have announced that they want to discontinue it, at least from 2022. So that is one of the big things on our radar. And then, yeah, challenges. I'm thinking about opportunities as well.

Interviewer 1:38

Opportunities is also an interesting aspect. You can also, you know, elaborate on that.

Morten 1:47

So you could take cookieless future, it's both an opportunity and a challenge. Because it's also adjusting more to what GDPR is asking of marketeers and the fact that you can't really? And it's the whole personalization talk, right? We've been talking about this as well at work. It's a difficult one. Is it possible to personalize without cookies and with GDPR? And does it even make sense to do personalization? Is it worth the effort? That's a talk we all have internally. As you know, Gabi, of course. And with this cookieless future, it is a challenge to do personalization, but we have first party data that we're collecting and we can utilize that. But

because of GDPR that's still in the same direction as a cookieless future, you can't really point out an individual and market to them so it will be more of this audience pooling that you will have to look at and target. Which isn't a bad place to be in. Because that is in some platforms, where we've had to be in anyways it simply isn't possible to add first party data or really utilize it in a big scale way. So we have to use more contextual targeting. And it's also about talking about platforms. What kind of data do they collect in general? And how much do they offer you to use as a marketeer as well? Google has like the vast amount of that, right? They have the search engine, which is a big pool of data. So if you could be honest, you could say it's easy for Google to release cookie data and go cookieless because they pretty much can collect that data in anyway through what people are searching. We can see it and some of the work we're doing with for some YouTube, we can build the custom intent audiences and stuff based on searches and what websites you're visiting. But yeah, it's been an interesting journey. I've been working with this now for the last six-seven years and it's interesting to see how it started out with them focusing more and more on targeting the individual and giving an individual an ID and using that. So the European Union talking about how they don't really want to see that development and introducing GDPR. Then rolling out GDPR. And now seeing that they closed all of that down. And it's going into this other direction of being poolling people together and, and not being able to point out an individual that says, of course, there's always a CRM, where you have an email addresses, and you can choose to direct mails to that individual. But what you see there as well as you might write the name, like Hello, your name, insert that. But it's still a pool of people you are targeting the same message for right? So to that degree it's not necessarily a personalization as such, not necessarily like, this is you, this is what we offer you specifically. But it also depends on the industry and the vertical and usually I'm thinking about Bang & Olufsen only, not that much into other verticals. And for us, it's dividing it into product categories, primarily, and we have some different audiences to work with there. And yeah, I know, we also, I don't know how much we've been talking about our company with Amanda. But we also have products that go to high net worth individuals. And that's also a discussion how to reach those because there you want to go personalized. But we also know that they probably buy out of getting advertisement. So that's a whole other ballpark on how to handle that and even if it's possible to do that digitally. Or you need to get into assistance or concierge

services and stuff like that. And would it make sense to market towards them digitally or reaching out in a more because that's a B2B kind of advertisement. Right? So it's something a bit different.

Interviewer 7:10
That's a specific challenge we have in Bang & Olufsen context. Morten, you actually touched upon so many things we want to elaborate on. But let's start with you mentioning first party data. So what role do you think first party data will play in the future?

Morten 7:25
I think it will play a much bigger role than before, especially because of a cookieless future. And it is the big rave now, when you look at what the different agencies are recommending you to do is going through collecting first party data, binding it to your CRM database. And using that instead, and actually also shifting some budget over to CRM, to mails instead, because it's more difficult to reach on an individual level for other digital channels.

Interviewer 7:34
And do you think all of these changes will have some kind of changes for your work in the upcoming 5 to 10 years as a manager, as a marketing expert?

Morten 8:34
Cookieless to some degree, I think, you know it, we weren't that big on personalization anyways. So I think for our type of company, it's not a big problem, to adjust to this. And we were already looking more into contextual targeting. Also, to make sure that we have a big enough audience to talk to. I think it depends a lot on where your brand is at and where you want to go with it. For us the brand awareness is high in some markets and low and others. We work with these six core markets where two of them, especially one - Denmark, where our brand is from, we have really high brand awareness. So in that market, we can go more into utilizing first party data and maybe be more specific on smaller audiences. But in other markets where brand awareness is low, we might want to focus more on bigger pool of audiences. And there first party data might not play as big of a role. So in that sense, it's also

up to where you're at as a brand and what is the focus of your marketing. But saying that there's always talk about how much should you split between awareness and tactical acquisition? Yeah, precision marketing, if we talk about specifically that, then yes, first party data will play a big role and you should utilize that as much as you can. It's not available on all digital platforms and as you know, it can be difficult to handle first party data on the platforms and being sure to updating it correctly. Because ideally, following GDPR, you should update it real time or at least daily. If someone opts out, then you need to remove the data quickly, or you could get fined. So, in that sense, there's, yeah, we're already working on that. I think it's more about the digital landscape, how that is shaping, and how Corona has changed it to some degree and about still doing a full marketing mix. And again, that also comes down to what is your goal for your brand? What makes sense for your brand? For us, it makes sense to do a bigger marketing mix because we have stores. If you're only an e-com web shop, then it might not make sense to go beyond digital marketing.

Interviewer 11:41
Okay. That's an interesting point. And we touched upon, you know, these emerging new privacy first solutions. So some of them include, you know, tracking free browsers, other solutions are currently being developed by Facebook and Google, that prevent, you know, this individual user identification that you've also mentioned. So have you discovered any privacy technology solution that you think could become an industry standard?

Morten 12:11
Like tracking people in any way?

Interviewer 12:14
For example, because basically, it's unavoidable that we will not have cookies anymore. It's unavoidable that Apple iOS update is coming. And various companies, various platforms are developing technologies, how to go around this, you know, and either that is differential privacy, if you maybe came upon that term, or just the whole Google privacy sandbox. So what do you think? Where do you think the industry is moving? And what might become the industry standard?

Morten 12:45

I think it's a difficult one. Because even though they're saying they're removing cookies, right, then they're trying to trick in other ways. So you could also argue, are we removing cookies, or we're just shifting to another way of tracking people? It's making it more difficult for people to understand what they're using to track them. And still, it's interesting that Google is still collecting a lot of data that I don't think they are transparent about. And Apple is just taking that step. And even though I think it might be just a smokescreen from Google's part to say, okay, we're removing cookies, but in reality, they are probably tracking a lot of things that people are not aware of and they're just not mentioning that. So, it's from a personal point of view I'm saying that, that's not necessarily professional. Because personally, I prefer that it's being more transparent and it's an option for you. And it should be that you know everything that they're tracking, and you can opt out if you wish to. And there was actually not an anecdote, but a situation when talking to Michael, our new marketing manager. He was saying that he actually closed down his Facebook account and used ad blockers and everything at one point, and then he understood how valuable actually it was to give up some consent, because the ads he was getting were just way off from what he was interested in. So he also, you can say, was annoyed with being advertised wrongly. So it's about maybe understanding that it can be difficult to understand on personal level, that you actually maybe want to get some more relevant ads. But at the same time, I'm opting in usually, and I'm still getting weird ads, that I don't understand why I'm getting, so it's a difficult playing field. And as we talked about Google, it sometimes puts you into these weird pools of audiences. Where like, that makes no sense that I'm in that pool of audiences. So yeah, going back to what you said - no, I haven't found like one new way of tracking that I think is kind of like the way to go, I think what we might get into is it being difficult to create a privacy policy, because all of a sudden, maybe they'll all do their own way of tracking data. And you'll have to make sure that you write that in your privacy policy. So from a legal point of view, it might be very difficult for them to start editing the policy to fit of the new ways.

Interviewer 15:58

Yeah, it's another challenge.

Morten 16:00

Especially when it's outside of iOS because Apple was just making it, fully transparent there and they have closed down cookies, it's only available for 24 hours, and that's opt in all the time. But both from a professional and a personal point of view, I think it's super annoying that you have to accept cookies, privacy policy all the time. I think there will have to be, in the next couple of years, I think there will be something about that. Because that constant popping up about being asked about that. I haven't read like someone really raving about it, saying that, that needs to change or anything, but I'm sure that consumers are a bit fed up with that. On a personal level thing, it's good, I can opt out. But it's the same website, you visit all the time, and you still keep saying okay, I except, I do not except. So it's annoying.

Interviewer 17:02

There's a phenomenon called privacy fatigue that we're also researching. So this thing you're talking about refers to that. Okay, yeah, everything is very interesting. And now maybe we could move to the findings that we already gathered. And we would like to, you know, receive your opinion on that. So, firstly, you know, we conducted this experiment where respondents were asked to share their email with a fictional online shop and get various benefits in return. And one of them was personalization. And as a result, we actually found that personalization has a negative effect on respondents' willingness to share their information. So why do you think that is?

Morten 17:45

Yeah, it's really interesting, because that's also what we what I touched upon quickly. You probably want it, but if asked for it, you don't want to say that that's what I want. Because I think you're afraid that you're sharing too much personal data, like it's maybe it's in the wording as well, like personal like, it's your personal space. That might be the point of it. So I don't know if you phrased it differently. But it's also how would you phrase it then, because it is about you specifically as an individual getting this offer. I think it might also be because of GDPR and all of these talks about tracking and the whole Apple situation - it's gotten a lot of traction in the news, right? So people are getting more aware of what kind of information is

being tracked of you. You think it's actually a couple of years ago, there were some what they call documentaries, or investigating journalism around it, as well. I think it was on, I don't know if he only asked in Denmark, but in Denmark and on some of the bigger channels I think there's actually the public service channel that had some investigative journalism on it. But also whistleblowers, showing exactly how much data that different companies were collecting on you. And it was quite surprising and also scary. Like there is a big focus on individuals with all kinds of data.

Interviewer 19:33
Yeah, I see what you mean, people just might become afraid of personalization. We as marketers kind of see it as a goal, right? It's usually the golden standard to provide personalization. But even the keyword itself might not seem very attractive to users. Am I correct?

Morten 19:48
Yeah, you're correct. And I think it might also be just a mental misunderstanding, because if you really understood that it's also about having interest for a brand or product, that personalization is also getting you the right offer at the right time. So it's making it easier for you as well, not to investigate but get this offer.

Interviewer 20:16
Yeah, that's very interesting, actually. And you briefly touched upon it, but like, do you think that personalization should be the aim of marketers? In general.

Morten 20:27
In general it's what we're talking about, right? Like the right message at the right time. And then you would expect the customer or consumer to to take action on it, right. So to some degree, you would call that personalization, right. I think there's different levels. There's also just think personalization is also a bit lower in the marketing from where awareness is also sometimes about just making aware of the brand and telling the story. Yesterday I read some different articles and it's also interesting to see how many opposing opinions there is about

branding. And is it working or not working? Or is it more personalization you should go into or is it just going broad and then people would buy what they think fits at that time?

Interviewer 21:26
Yeah, the funnel approach.

Morten 21:27
Yeah, there's a lot of opposing opinions on that. I know a lot of agencies and that it is really being pulled up a lot, in terms of going broader and saying that branding is not really working, and personalization as well. It's all about just getting a brand out there to as many people and then they would buy it. I'm not saying that I agree. I think building a story about a brand is important and it is influencing people's decisions. That doesn't necessarily say anything about personalization.

Interviewer 22:17
Yeah, okay. Well, actually, we had an interesting finding that even though respondents were very concerned for their privacy, as you're saying the awareness is quite high in this area, they were still willing to share their data if the value they gained in return was sufficient. So as we mentioned, personalization benefits were not enough. But in your opinion, what value should an online shop offer its users in return for sharing their personal data? You know, what should the shop, the vendor, just offer in exchange?

Morten 22:56
Yeah, it's interesting. I think, a lot of e-com shops and brands in general, are using incentives to offer something in return to get signups for example newsletters and get their data. I don't think that that should be enough necessary. Because then you risk that they actually just opt out after getting that discount. So I think, I don't know. I haven't read anything about it. But I would guess that a large portion of people would be discount hunters or something in that sense. And if you get a discount by signing up, then you would probably opt out the quickly again. Also, personally, I've done that. It's a way of just getting a discount and then removing your data from that brand or shop. Again, I think, ideally, you should build a brand instead

with a story and get people involved and interested in actually buying from you. But it might also be difficult because if your shop is without a real brand. But anyways, just utilizing discounts on your shop to get people to buy from you, which I think is a big thing, especially in Denmark, we are really bargain hunters, the Danish people, our culture, that I have read a lot of articles about. And I think that's why a lot of shops are really using that. So in that case, I would say you probably need that. And then you get people hooked in the loop of getting newsletters with "this is the discount now and look at our offers". And I actually think especially in the Danish culture that you would get people hooked and you can use the data in a useful way. From the Bang & Olufsen standpoint, for example, a luxury brand where we have a price policy and we don't want to do discounts - you shouldn't use them. So it's more about building the brand. And yeah, the luxury, I would say, don't use incentives. In fast moving consumer goods, I would say it could work. I haven't worked that much with it. But I think, from what I just said, incentives could work.

Interviewer 25:34
Yeah. And as you're saying, probably in combination with branding and engaging users, right. So it wouldn't be just a short term gain of opt in.

Morten 25:42
No no, yeah, you should still keep like, so your brand as a shop would probably be, we are the discount shop, right? We are the cheapest one for you to always choose. That would be kind of like your branding, as such. That's something I find interesting, but it's also a way of making your mark. Yeah.

Interviewer 26:04
And actually, previously, with some previous people we interviewed, we heard a keyword "trust" being mentioned when talking about people being willing to share their data. Do you think that's an important factor?

Morten 26:17
Yes, absolutely. I do think, but how do you build that with small ads about signing up?

Interviewer 26:24
That's the question, how do e-shops build trust? How a business or a brand can build trust?

Morten 26:33
I think it's about using the, you know, Trustpilot and these other recommendation sites, recommendation portals. A lot of e-commerce shops are using that right in their marketing to show that people trust us, give us good reviews. But that's also service based. I think service also like doing a good service is also building trust for you as a user or consumer. So I think that would be the most important ones. For us, yeah, it depends. Now, we I'm thinking about like fast moving consumer goods when I'm saying that. Sorry, about Bang & Olufsen, for example, I would say it would be also service reviews. Yeah, I think we've performed short on some things. Because our service hasn't been at the level that we wanted, you know that. Well. I think as a luxury brand, we will need to accelerate, to get to a point where people feel that they're getting the correct service. Because buying into luxury is also buying into service. You expect when you pay a certain premium, then you will also get a premium service. So that is really important.

Interviewer 28:20
Okay, and maybe more than just for an extra minute of yours. Just to wrap up the discussion. What do you think will be important for businesses trying to adapt to this privacy first world?

Morten 28:38
I think the difficult thing is GDPR is still a bit fluid, right. And it differs how much companies are adhering to the rules. I know we are trying to be strict and follow them pretty much on the strictest terms. Whether or not that's a good thing, it can be discussed. But I think it's important, you should adhere to it as a company. Also, because, as you say, your findings might prove that it is on consumers radar, it's something they're thinking about. And think about the data. And maybe at some point, they would get to a point where they would start to opt out from companies asking them to delete the data if they don't trust them. So investigative journalism is still big, right? And if there are brands that are getting hit by some

of those investigative journalism articles or TV shows or anything, that they might see a surge of people opting out from their data pool, I think that could be a pain in the future.

Interviewer 30:06
Like reputation is very important in this.

Morten 30:08
I think reputation is a thing, yeah. Otherwise, yeah, being transparent as a company, super important. But that's always been my opinion also in terms of having a trustworthy brand. And yeah, reputation as a part of that as your brand.

Interviewer 30:32
Okay, Morten, thank you very much. Your answers were incredibly useful.

Appendix J

Interview with Thomas Bering, 2021.04.22

Thomas Bering 0:00

Yes. So I'm Thomas Bering and I have been with Google since January 2005. So just over 16 years, and since the first of April, I am the brand measurements, full funnel lead for the Northern Europe region, and also sort of possibly still the privacy lead for Denmark and for the last year or so.

Interviewer 0:25

Okay, very cool. What does it mean to be a privacy lead? Exactly? What do you do?

Thomas Bering 0:30

It means that Yeah, that's a good question. It means that I try to tell the Danish team at least what's the internal.. What sort of moves we're making internally, and try to hopefully make them understand how it affects them and their discussions. So try to translate the internal developments to something that they can take out to customers. Okay.

Interviewer 0:57

Sounds really cool. So yeah, as I said, we have 10 questions. And the first five questions will be around the different trends we have spotted around data privacy. And afterwards, we will jump into an experiment that we have conducted, Gabi and I, and we want to discuss the results we found actually with you. So yeah. In the beginning, we want to ask you, what do you believe are the biggest challenges for digital marketers right now? And how would it affect the industry?

Thomas Bering 1:29

I mean, the easy answer is that the loss of cookies and tracking and everything are the biggest challenges. That I think I also feel a bit of a boring answer. So I'll try not to stick to that, to me, the biggest challenge is facing the unknown, to be slightly more philosophical. The biggest challenge is that anyone who's worked with digital marketing for any amount of time

for the last 5-10-15, maybe even 20 years, has been used to being able to measure everything, and all discussions and planning has been around, moving closer and closer to the personalised marketing, the one to one discussions and all these different types of things. And all of a sudden, that entire Foundation has been ripped away from them. So obviously, there's a large technical void. But that is not a problem for the average day to day marketer. The problem for them is to say, okay, so with what we have right now, what can we do? So, so to me, the biggest problem is the mindset shift, is that everyone who has been raised to do digital marketing or learn anything about digital marketing, needs to be able to rethink, okay, why is it we're doing marketing? What, what can we do now, because for most of us, me included, we're not making the decisions, we're not changing the technology, we can have our opinions about it. But none of us are going to change it, what we can do is adapt to it and try to use it as best as possible for the best results. But that requires a change in thinking. So that, to me, is the biggest challenge.

Interviewer 3:13
So what do you think will be the biggest change for your work in five to 10 years?

Thomas Bering 3:18
Oh, Crikey. Five to 10 years long,

Interviewer 3:21
we can start with five years.

Thomas Bering 3:23
Since that makes it easier. I think the the biggest change will be for me, personally, I think it will be more interesting, because the more you go into one to one type of thing, the more also you've things fall into noise and chaos and all these businesses. I mean, I've sat in some meetings where people have asked us for data, where you're thinking, you can never use any of that data for anything. So I think it will make the biggest it will mean I think, I think my job will become more interesting because more of the above saying Okay, so there's, instead of impossibly imagining that we have 1000 different customer segments actually only have

five, but we can make them really good, because this is where we have some insights and some data. And we can tell for instance, with Google data on conversions with Google first party audiences, for instance, will actually our ROAS is five times better for customers who have an affinity for green living, for instance, good. That means we can build creatives around green living, that means we can inspire our creative agency to build better ads here. We can use that in the product development. We can value these segments and spend more on them. So in some ways, it's going to I think it's going to make my job more fun because it's limiting to some extent, the scope that people can work with, which means that they can focus more and I think that will be very interesting. Hopefully fun.

Interviewer 4:55
Hopefully, yeah. Okay, so we have noticed many privacy first solutions emerging right now, new tracking-free browsers, differential privacy, FLOC technology, it's only to mention a few. What do you believe could become an industry standard?

Thomas Bering 5:14
I think I coming from where I do need to be very careful in answering that question. To be honest, as well, just to make sure that that's on the record. So personally, I think is also the disclaimer I need to put in there. Personally, I don't think there will be an industry standard actually is my completely honest answer, I think the standard will be more first party data. So the standard will be businesses being better at picking up their own data. So if I don't know that, that's an industry standard, but companies being better equipped to say, okay, we've now gotten these customers in, they have, they trust us enough to give us this information. Regardless of regardless of whether we are Google or B&O. I have a better example, regardless of whether we're Google or Apple or Facebook, wherever we are. But actually, I trust my relationship with Bang and Olufsen so much that I want to give them this piece of these pieces of information about me because I know what they're going to use them for. And then Bang and Olufsen can say, well, we can see that our customers who buy the most are from 25 to 30. So that means we'll sell them this product and the one. So that means the people who are 25, or 30, that we haven't seen yet, we can send them this type of information, the ones who are between 50 and 60, buy less but more expensively, so we can send them

these types of messages. So I think the industry standard will be more focused internally in the business, rather than what third party offerings can offer.

Interviewer 6:45
Okay, so you're saying you don't think there'll be one industry standard? Do you believe that for example, the FLOC technology, will it be beneficial for users? Or will they even notice a difference from the cookies?

Thomas Bering 6:58
I was about to say your second assertion there, I don't know that they'll see a difference, I think. And again, this is, I think, formally also very much a personal opinion. We give a lot of ads, transparency, insights, anyone can click on the eye to see why they're being shown this ad, you can do the same on Facebook, you do the same on most platforms. I think the average user doesn't use them. But those of us who are in the business, we think that everyone is interested, to be honest, no one really cares.

Interviewer 7:30
Yeah, before we jump into what we've actually.. we have conducted an experiment where we also found out the same result that people say they are very concerned with their privacy online. But when it comes to show, it wasn't really that important for some

Thomas Bering 7:45
If you see an ad that's really relevant for you you're interested in, if you see an ad, you don't care about nine times out of 10. You just ignore it. You don't even get upset, sometimes you get upset, but the average user, they just want to read the content.

Interviewer 7:59
Yeah. Probably quickly, scrolling away finding something else to look at.

Thomas Bering 8:04
I mean, I shouldn't say that, because it pays my bills. But But yeah.

Interviewer 8:11
yeah, so I just told you about the experiment we have. And we saw that people are very concerned with their online privacy. They said at least. And they also believe that the internet provides serious privacy issues. So why do you think that they say that kind of comments, why do you think that they claim to be very concerned with that data privacy?

Thomas Bering 8:35
Well, I mean, partly for good reason. And again, I'm being cautious in my answer here. But partly because there are some concerns, and there have been cases where data has gotten into the wrong hands and meant that internet banks could be exploited. That's real, personal impact could be felt. So anytime you have a case like that, I would be concerned about my privacy as well. I'm obviously keen that my bank details aren't shared that people don't start syphoning off money from from my bank that, but I think the problem is that conflates into the challenge of more general privacy, I agree that there should be privacy. I believe that users should be able to control which things are stored about them. But most users being careful, but I'd still argue most users don't really distinguish between someone broke into my internet bank and someone knows that I'm interested in tennis shoes, that that it's it happens online. So therefore, it's part of the bigger privacy narrative. So it's easy to point to these great big mess failings, and say That's the problem with privacy on the internet. Where actually no, that's a bit like saying someone crashed in the car is the same as somebody tripping when they're walking on the sidewalk. Yes, it's a means of transportation. But it's actually two completely different things. That's possibly the worst analogy of the week, if not the month, but I think hopefully you get the idea.

Interviewer 10:21
So how do you advise clients on earning the customers trust?

Thomas Bering 10:28
Hmm. So we are in the fortunate position, to be honest, that we spend less time on this. It's not really I mean, to be honest, especially in my role, we sell ads. So so

Interviewer 10:42
famous Mark Zuckerberg quote, also.

Thomas Bering 10:47
Yeah. And it's, it's so so I mean, obviously, we're interested in, in business being able to pick up data because if, with more and more cookies being said, No to if they can't use conversion tracking, then they won't be able to track so we're interested, of course, so. So that was only a slightly sarcastic answer. But the other side is we can't really, we can't advise anything legally, as well. So the things retail businesses are, we can't tell you how, but you need to get your customers to trust you. And everyone has been looking quite rightly towards us towards Facebook and Google and these others for a long time. But at the end of the day, if it's being B&O or Coop or the small local pet shop, who fails on privacy, then the finger is going to point at them as well, that it I think for a long time, largely also in Denmark, businesses just say, Oh, it's a big company problem. But now it's everyone's problem. So they just need to build up trust, they need to, they need to be sometimes, kindly, sometimes less can be reminded that businesses are there to serve the customers, not the other way around. That this idea of what you're just going to give us your data. Of course you are, and we're not going to give you anything back. That is so 20th century type of thing. But most businesses online still seem to believe, you know, you should just tell me everything. And then I'll find out. So there's this feeling that more data means you can do more things, but really, a most businesses that that even I work with don't use that data for anything they have. Some have massive customer databases, and they don't use it for anything. And that degrades trust. And then on the other hand, if you ask for for nothing, then you have nothing but you said, Yeah, I generally don't advise. But when I do, it's about saying well make it clear why you're asking for what you're asking for. If you need an email, just send an email. That makes sense. If you need my physical address or birthday to send me an email. I'm just gonna, I'm gonna question that. Unless you give me a good reason again, then all of a sudden, you say, well, it's, I'm Carlsberg. So we sell alcohol. So we have to know you're over 18. Okay, fine, then that makes sense, then I can see why I have to deliver this information. It's good. It's explained why you're doing it. And I think I'd like to think in Google, we're relatively good at that. And

people can see, okay, well, if I allow you to understand what I've previously searched on and make my results better, that's fine. If you don't want that, then you're still going to get good results, just maybe not as good because we can't make them as good. But again, if you go into a bar, sorry for using the alcoholic expression plus, we can start going in I mean, I even wrote a piece on it for something, if I go into the globe, which is the Irish Pub. Just up the street from the office. I've been there for a long time. So if some of the people have changed, but for a long time, they'd start pouring a pint of Guinness the second I walked in the door, because yeah, I'm an alcoholic. Oh, yes, that's the word local. But so when I go in to the globe, and they start to pour me a pint, it saves everyone time. And they I know I trust them with that information. I don't, they're not going to be even if they did tell everyone I don't care where it saves me time. So it's Convenient, I don't have to think about it. So they're also certain that I will take that point. Because even if I came in there and was thinking, Oh, I'll make just have a glass of water today, I'll probably say I just just the one then. So everyone wins. And I think that is the is the other part of why people are so concerned. And again, it's it's my personal opinion that I have to be somewhat careful that people also have this idea that they are the most important person in the world. And yet, unless you are Bill Gates, or Joe Biden, or whoever the individual data of an individual person means next to nothing.

Thomas Bering 15:44

From the business models that most advertising companies drive, you earn so little off of one person. It's only when there's 1000 or a million, then it actually starts to add up. So everyone wants to feel that they're the most important person. And they are important. But ask a big company, what would happen if you took out one of these people? Nothing. So again, this idea of all the big companies can see who I am. We can't either do that option doesn't really exist. But even if even if I could go in and see what either of you were doing, it wouldn't wouldn't add any value, it wouldn't give me anything, it wouldn't help in any way will make the product better or worse, because we cannot tailor products to individual people, we can tailor to groups.

Interviewer 16:38

So experiment we conducted, we created a banner where we ask people if they wanted to share the email with us, and to get the personalization benefits in return. And the result we found was that we actually found it to have a negative effect on their willingness to share the information. So why do you think that is? They were not willing to give out the email in returns of personalization benefits.

Thomas Bering 17:05
Well, what were those benefits?

Interviewer 17:07
Yeah, so the banner only included.. it was very vague. So that's kind of the point of the experiment we wanted to see. Okay. Do people really like how can we trigger them in some way? So we just said that they could get their style tips and the and the, like, emails tailored specifically to them? Yeah.

Thomas Bering 17:27
And yes, so that would be, that would then be my best guess as to why people wouldn't if you don't have either an established trusted brand, or a really, really good value proposition and they sort of counterbalance each other, then I think people are smart enough Luckily, to say, I'm actually not comfortable. And I don't I don't I don't even know if that's privacy, or just the frustration of spam is just I don't need my email to go out to yet another place gets 20 emails a day with products I don't need. Okay.

Interviewer 18:06
And we also found that even though our respondents were concerned with their privacy, as we talked about before, they say they were still willing to share that data if the value they gained in return was sufficient. So personalization benefits were not enough, as we just said. Okay, so, in your opinion, what value should an online shop offer users return of sharing the personal data?

Thomas Bering 18:31

Oh, that's an interesting question. Um, so I would disagree with your phrasing that personalization isn't enough. I think, in the right context, personalization is enough. If it were B&O, I might actually give it because I trust them if they're going to tell me something cool. I'll happily sign up for that. If it's Amanda and Gabi's happy showroom. I don't know who that is. I'm not I don't trust them enough to give out any information yet. So I think it so we've just done actually a really interesting case study called decoding decisions, where we use behavioural science to analyse what drives people from considering different brands to taking the step of actually purchasing them. And analysed and I I'm also sort of the spokesperson for Denmark for that. So I should be able to remember it better. But there's six different cognitive biases, which we found to have impacted that decision making process significantly. A number of others of course, but but some of them were things like social norms and category risks and social norms, of course, being things like if you could say that on trustpilot, this has five stars or everyone loves it or 400 users are happy or whatever. And cognitive heuristics being things like for cereals, whether they're high in fibre or organic, for instance, we were able to test some of these different messages and find that getting the messaging, right had a significant impact on whether or not people would choose that brand. So I think it's it there, it's going to vary for every segment. And it's going to vary for every company. But I think there are some things which will drive people more than others. And I've studied English and philosophy. So I really don't know very much about it. But the whole area of behavioural economics, I think, is starting to come up. But it's still overlooked. And I think that is what will, what can drive these things as if you get the messaging, right. And it's small things and sometimes people aren't even conscious that it is that one small thing that makes a difference. Maybe if you and your banner had written personalised tips for an organic lifestyle or for a minimalistic lifestyle or for whatever what was an A Marie Kondo lifestyle or something that would be the little trigger that will get more people to sign up? So it's tweaking. So so. So that's the one side and I think your actual question was what they could offer a value. That's almost it's not secondary. But they can have that value. But if they don't communicate it, then it doesn't matter. So they can, they can use the messaging to find out what the value they should be offering is they can be looking businesses should be looking at their competition almost every single day to find out why are they getting these

customers that we aren't? What are they offering that we don't have? Is it same day shipping? Is it free returns is it's organic? t shirts, whatever? Okay,

Interviewer 21:43
is it something you could share with us? Like, is it confidential? Are you allowed to share this?

Thomas Bering 21:47
I think you I think you can search search for decoding decisions on think with Google. So

Interviewer 21:52
I'll write that down.

Thomas Bering 21:54
We've done we did five verticals in Denmark, I think we did 20 or something in the UK, we've done some for Sweden and the Netherlands as well. But but very consistently, they just yet analyses, six different jurisdictions and looks at even even even the fact with the way we did set up, I'll give you the very short summary. We ask people what their favourite brand was, who were in market for a product in Denmark, we tested mortgages, moisturiser, cereal, mobile networks, and

one other.

Four out of five is not bad. And and then said, Here's your favourite brand, would you like it? People would say yes. And then even we present them with two different options, number one, and number two, and in most cases, somewhere between 20 and almost 40% would actually choose number two, just because it was there. So even though people have made an expressed interest in number one, just by giving them a second option, they would choose that. And then we started to tweak the messaging to sort of play with people's minds. And then we were able to convincingly pull them over to the second brand by tweaking the biases, and then we introduced a fictitious brand. And so obviously, no one had heard of it for cereals

that was called God Start. And then presented that as an option. And again, somewhere to 20 to 30% would choose that, because it was there. And because they had the right messaging tweet.

Interviewer 23:19
That's so interesting. We will do the research there and see what that's all about. Because that's so relevant for our thesis as well.

Thomas Bering 23:26
Yeah, you can download this white paper to making what is it making sense of the messy middle?

Interviewer 23:33
Okay. Perfect. Thank you for an amazing tip here.

Interviewer 23:47
you are giving us a lot. This is so good for our paper. Finally, we have one more question. Let me just see if there's anything I'm missing. Yes. Okay. So this one is a little bit of a bigger question.

Interviewer 24:06
I think this is a little bit bigger because it kind of gives more room for reflection here. So what is your advice to businesses trying to adapt to these privacy first standards?

Thomas Bering 24:27
Yes, that is bigger. But I think on the other hand, it's it's I mean, the really simple answer is accept it.

Interviewer 24:39

accept it

Thomas Bering 24:41

because I think there's sort of different parts implicit in that, but I think the main implicit one is another ad actually goes, whether it's a business or an agency or anything, it's just this is not like the Super League. This is not going away in 48 hours. That's really bad. analogy. But I've been very, very taken by the Superleague over these last couple of days in the complete idiocy of the whole undertaking. It's just my opinion. But but we still see some businesses sort of sitting back and saying, No, no, we have all this data. And we're going to have to keep doing this. And we still get questions on some good help. But how can we keep tracking this way? And just have to say, Well, you can't, but we have to, but No, you don't. Because you can't, it's like saying you still want to ride your horses on the on the motorway, but you're just not allowed to because we have cars now. And so, so roll with it. And so there's, like I say, like, I think I said in the beginning, there's a number of technical elements to this, which are going to be required, and they're going to have to look at their data differently other grant to do better at collecting it. Agencies are probably going to have a bigger role to play in regards to pulling data in from different sources, because it's going to be more disjointed, all those things. As I say, to my mind, they're sort of the boring technical answers, the main challenge is going to be in the psychology of these companies saying, OK, we're going to have to do something, we're going to have to take this next step to find out what happens here. And the companies don't have the answers. The agencies don't have the answer. Google doesn't have the answer. Apple doesn't Facebook, no one has the answers. But all we can do is say okay, well, we can sort of see a few months into the future, we can set up some benchmarks. Now what I think the maybe more constructive answer is businesses should be looking at setting up some form of benchmarks, so that they know we have 1000 customers today, next year, we'd like to have 1200, we don't, we're not going to know where every single one of those customers came from. But we should have some pretty good ideas. And so we're going to have to pull in all these different insights. And then we're going to in two years time we'd like to have 1500 customers, well, we got these 200 incremental customers by doing these things. What if we do the same will that give us 200, more or 300 more, if it gives us 200? More, we can say, Well, this is the strategy for getting 200 customers, we'd like 300. So we need to

tweak and tailor some of these things. And so being much more willing to accept the fluidity, if you will, of the situation and test an experiment. But knowing what it is you're testing and experimenting, because that's the other problem is people will say well give give, we're panicking. So give us all the data you have. So we can crunch off that. No, you don't know what you're looking for you we can give you or we can't but even if we could give you all of the search data on every single user in Denmark, what are you going to do with it? And it's not in Denmark, but I have genuinely had that request from a large Nordic customers. We'd like the search data of every single customer who visits us from your site. And my first thought was, Why? What are you going to do with it? And they couldn't really answer but they're like that, that would be really valuable for us to have? No, it wouldn't. Just Honestly, it wouldn't.

Interviewer 28:10
Oh, did they explain why

Thomas Bering 28:12
they didn't really have a good answer for that. Other than that they were data hungry? Yeah. That's that was not their word. That was my

Interviewer 28:21
that's the thing.

Thomas Bering 28:22
My very active conscious thinking of, but that so so there is that danger. And I think it is a real, very real risk that many businesses are running is that they they feel the only way to cover these gaps is by having more data and which is also why there's a degradation of trust and a lot of businesses because they ask for so much better ask better for 10 things and then only use three whereas they actually know what if you What if you only ask for two and then you realise you need the third one is people trust you enough, they will give you the third piece of information. Rather than saying Why have you asked for all these 10 things when you only need three of them?

Interviewer 29:00

Really good point. I can see we're also running out of time and we have no more questions left but it's amazing interview really. We have so much to dig into now. Do you have anything on top of your mind Gabi or did we get it all.

Interviewer 29:16

honestly just trying to digest everything that was said here and really looking forward to analysing all of the gathered here more in depth.

Thomas Bering 29:25

And I look forward to hearing the interpretation of what I've said hopefully it was useful.