Tampereen yliopisto

Jere Laine

THERE IS NO DECISION: DESIGN OF COOKIE CONSENT BANNER AND ITS EFFECT ON USER CONSENT

Faculty of Information Technology and Communication Sciences
Master's thesis
November 2021

ABSTRACT

Jere Laine: There is no decision: design of cookie consent banner and its effect on user consent
Tampere University
Master's Degree Programme in Information technology
Master's Thesis
November 2021

After the European Union introduced the General Data Protection Regulation and Directive 2009/136/EC websites have been obligated to ask their European users consent before placing cookies on their device. As an adverse side effect his has led to a situation in which most websites now feature a cookie banner. Constant consent request have led to a phenomenon called "cookie fatigue" where website visitors no longer take the time to understand what they are consenting to due to the high number of consent requests.

The study explores how humans make decisions when facing a cookie banner and if the decision is made in such a way that the consent can be considered valid. The work is divided to three stages. First, fifty Finnish websites were visited to gather information about what kind of cookie banners are commonly in place. The second stage describes how a test website and a cookie banner with variable button colors, button layout and text options was created utilizing the information collected in stage one. Finally, the third stage consists of a user study where this test website was combined with a questionnaire in an attempt to determine if and how these options affect consent rates. After this, an attempt was made to explain any observed effects.

Based on the results of this thesis a significant number of people do not seem to pay much, if any, attention to what they are consenting to when facing a cookie banner. The color scheme of the buttons to accept or reject cookies was found to be more significant than even drastic changes in the amount of information collected using cookies. Also, the overwhelming majority of people who accepted cookies stated that they would not do so if it was possible for them to reject non-essential cookies using browser settings. This might signify that people have been conditioned to accept cookies, as nothing else that was discovered can fully explain this contradictory behavior. The location of the buttons was found to have no effect.

Finally, the thesis makes suggestions to policy makers to alleviate the issues and prevent them from resurfacing again in a different form.

Keywords: cookie banner, nudge theory, dark pattern, cookie notice, cookie pop-up

TIIVISTELMÄ

Jere Laine: Päätöstä ei ole: evästebannerin ulkoasu ja sen vaikutus käyttäjän suostumukseen
Tampereen yliopisto
Tietotekniikan tutkinto-ohjelma
Diplomityö
Marraskuu 2021

Sen jälkeen, kun Euroopan unioni otti käyttöön yleisen tietosuoja-asetuksen ja direktiivin 2009/136/EY, verkkosivustojen on täytynyt pyytää eurooppalaisten käyttäjiensä suostumus ennen evästeiden tallentamista heidän päätelaitteeseensa. Ikävänä sivuvaikutuksena tämä on johtanut tilanteeseen, jossa useimmilla verkkosivustoilla on nyt evästebanneri. Jatkuvat suostumuspyynnöt ovat johtaneet ilmiöön, jota kutsutaan "evästeväsymykseksi". Se tarkoittaa, että hyväksymispyyntöjen suuren määrän johdosta verkkosivukävijät eivät enää jaksa selvittää, mihin he antavat suostumuksensa.

Tutkimuksessa selvitetään, miten ihmiset tekevät päätöksiä kohdatessaan evästebannerin ja tehdäänkö päätös siten, että suostumusta voidaan pitää pätevänä. Työ on jaettu kolmeen vaiheeseen. Ensin käydään viidelläkymmenellä suomalaisella verkkosivustolla keräämässä tietoa siitä, millaisia evästebannereita yleisesti käytetään. Toisessa vaiheessa kuvataan, miten ensimmäisessä vaiheessa kerättyä aineistoa hyödyntäen luodaan testisivusto ja evästebanneri, jossa painikkeiden värit, painikkeiden asettelu ja tekstivaihtoehdot vaihtelevat. Kolmas vaihe koostuu käyttäjätutkimuksesta, jossa testisivusto yhdistetään kyselylomakkeeseen, jolla pyritään määrittämään, millä tavoin nämä vaihtoehdot vaikuttavat suostumusten määrään. Tämän jälkeen työssä pyritään selittämään havaitut vaikutukset.

Työssä saatujen tulosten perusteella huomattava osa ihmisistä ei näytä kiinnittävän juurikaan, jos lainkaan, huomiota siihen, mihin he antavat suostumuksensa evästebannerin kohdatessaan. Evästeiden hyväksymistä tai hylkäämistä koskevien painikkeiden värimaailmalla todettiin olevan suurempi merkitys kuin jopa jyrkillä muutoksilla evästeiden avulla kerättyjen tietojen määrässä. Lisäksi ylivoimainen enemmistö evästeet hyväksyneistä totesi, että he eivät tekisi niin, jos he voisivat hylätä ei-tarpeelliset evästeet selaimen asetusten avulla. Tämä saattaa merkitä sitä, että ihmiset on ehdollistettu hyväksymään evästeet, sillä mikään muu havaittu ilmiö ei voi täysin selittää tätä ristiriitaista käytöstä. Painikkeiden sijainnilla ei havaittu olevan vaikutusta.

Lopuksi työssä esitetään poliittisille päättäjille ehdotuksia jotka lieventäisivät ongelmia ja estäisivät niiden toistumisen eri muodossa.

Avainsanat: evästebanneri, nudge-teoria, dark patterns, evästeilmoitus

FOREWORD

This thesis was made at Tampere University, department of Human-Technology Interaction.

I want to give my thanks to my supervisor Iikka Pietilä whose suggestions, observations and knowledge of the field helped this thesis to become much better than it would have been in my hands alone. The support he offered has been exemplary and one could not hope for a better supervisor. I also want to thank Heikki Tolvanen and Elias Aarnio for their expert knowledge concerning cookies.

Special thanks to Tuuli without whom I would probably never have graduated.

Barcelona, 19 November 2021

Jere Laine

TABLE OF CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

Abbr.	Abbreviation
CMP	Consent Management Platform
GDPR	General Data Protection Regulation
IP	Internet Protocol
Traficom	Finnish Transport and Communications Agency
WCAG	Web Content Accessibility Guidelines

1. INTRODUCTION

Privacy is under threat. In recent years, the rise of online advertising has driven companies to develop more and more sophisticated systems for targeting advertisements at consumers. For these advertisement systems to be most effective, as much information as possible must be collected from the people who see the advertisements. While targeted advertising can be harmless and even useful such as displaying adverts of latest role-playing games to a known role-playing game enthusiast, they can also be used for more nefarious purposes. Election results can be influenced by targeting online advertisements to certain groups of people. Advertisements can also be used to spread misinformation to people who are the most susceptible to it.

In order to limit the amount of information that can be collected from individuals and to unify the 27 different regulations across the member states, the European Union passed its General Data Protection Regulation (GDPR) (Burgess, 2020). Other governments around the world have not been idle, either. In Thailand, a somewhat similar law called Personal Data Protection Act will come into force in 2022 (Leesa-nguansuk, 2021). California Consumer Privacy Act which is effective of January 1st 2020 (State of California Department of Justice, 2018) also has clauses similar to the GDPR.

These laws and regulations directly affect the lives of over half a billion people (Eurostat, 2020; Worldometer, 2021; United States Census Bureau, 2019). It is impossible to tell how many people are affected indirectly: according to recital 14 of the GDPR, as long as the data processor is within the EU the regulation applies to all natural persons “whatever their nationality or place of residence”.

With these laws the appearance of the World Wide Web has changed. Nigh on every European website (and non-European website with a significant amount of European visitors) displays a “cookie banner” since the website operators now require visitors to give their consent to storing advertising cookies on the users device. The GDPR has even resulted in the dawn of an entirely new industry: there are companies selling cookie-banners-as-a-service, such as Cookiebot, Cookie Information and Osano. These are better known as Consent Management Platforms (CMP’s).

But are these cookie banners actually useful? The GDPR came into force in May 2018 and these cookie banners have been in existence for three years at the time of writing. After giving thousands and thousands of consents, are Europeans still giving their informed consent when facing a banner? The

purpose of this thesis is to first determine what kind of cookie banners are currently in use and if the consent obtained using such a cookie banner can be considered valid. This is accomplished by performing an experiment in which test participants are asked to use a website with a cookie banner. User choices are then recorded. Finally, the results are evaluated to determine the most important factor behind user's choices.

This thesis contributes to (1) understanding how small changes in user interfaces can influence human decision-making, (2) how changes influence user behavior if left in place for extended periods of time and then removed and (3) determining whether or not a consent obtained by the use of a cookie banner is valid in a court of law.

This thesis starts with a thorough review of cookies in chapter 2. This includes a legal definition of cookies within the EU, motivations behind using cookies and what is a valid consent from a legal standpoint. Chapter 3 contains the theoretical framework that can be used to explain user behavior from a psychological standpoint. Research questions are covered in chapter 4. Chapter 5 covers the website review process including what websites were reviewed and why along with what conclusions could be drawn from the results. In chapter 6 it is described how the test website and the cookie banners designs were created and what technologies were used. Chapter 7 covers the empirical research process and its results along with its limitations. The final results, proposed changes in legislation, suggestions for future work and research ethics are discussed in chapter 8.

2. COOKIES

In order to fully understand the topic it is important to know what exactly cookies are (both technical and legal viewpoints), what are the motivations behind using cookies and designing cookie banners and how laws regulate the use of cookies and similar technologies both within the European Union and in Finland. Chapter 2.1. covers the technical definition of a cookie, while 2.2. covers the legal definition and, more importantly, what is a valid consent from a legal perspective. Chapter 2.3. describes the guidelines for using cookies in Finland. Chapters 2.4. and 2.5. discuss the benefits of using cookies from the perspective of website operators and website visitors. Finally, chapter 2.6. presents various reasons for why a website visitors might not want to accept cookies.

2.1. What cookies are

Cookies are small text files that a website can save to the visitors computer. The most important use of cookies is recognizing the visitor of a website. For example, after a user logs into a web service, the server can store an authentication token in a cookie. When the user goes to a different page within that website, the token stored in the cookie lets the server know that the user has already been authenticated. Without cookies (or related technologies) the user would have to input their username and password every time they go to a new page within that same website. For these reasons it is most of the time necessary to have cookies enabled when browsing the web. (Barth, 2011; MDN Web Docs, 2021a)

Cookies can be divided into two categories based on how long they remain on the users computer: session cookies and persistent cookies, sometimes also known as permanent cookies. Session cookies are deleted when the web browser is closed. Persistent cookies will remain for a longer period of time, possibly even years since there is no upper limit for the storage time. (Fiebrandt, 2018; MDN Web Docs, 2021a)

Cookies can also be divided into two categories based on the domain from which the cookie is loaded. First-party cookies are set by the website the user is visiting. Third-party cookies are set by some other domain. This is important, since cookies can only be accessed by the domain they are attributed with. For example, if a user visits example.com and that website sets a cookie on the user's computer, that is a first-party cookie. However, if that website loads a

script from ad.exampletracker.com, and this script sets a cookie belonging to ad.exampletracker.com then it is a third-party cookie. The main use for these third-party cookies is tracking the user across websites: anotherexample.com cannot read the cookies placed by example.com but if both websites use the tracking script from ad.exampletracker.com, that script can read the third-party cookie on both websites and thus track the user across the internet. (MDN Web Docs, 2021a)

It is important to point out that the European "cookie law", that is, the ePrivacy directive article 5(3) and the Finnish law implementing that directive, Information Society Code 2014/917 (*Laki sähköisen viestinnän palveluista*) 205 § apply to any and all forms of data stored on a user's terminal equipment. More of this in the next chapter.

2.2. Legal basis for consenting to cookies in the EU

As stated in the EU Directive 2009/136/EC which amends the ePrivacy directive from 2002:

"Article 5(3) shall be replaced by the following:

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

In the EU member states the laws concerning the matter are derived from this paragraph. As we can see, article 5(3) does not mention cookies at any point: it merely states that storing any information in an end user's terminal equipment is forbidden unless the user has consented to it. Finnish law implementing the directive in question is worded similarly and also applies to any data stored on the user's terminal equipment (Laki sähköisen viestinnän palveluista 2014/917, 2014). Therefore in the context of the law the term "cookie" can also refer to browser localStorage, sessionStorage, tracking pixels, fonts, javascript files and any other method of storing data on a computer that can be used to identify the user and track their activities online in some fashion. The same definition will be used in this thesis. In other words, unless otherwise specified

the reader may assume that the word “cookie” also refers to localStorage, sessionStorage, tracking pixels and the like.

It is worth pointing out that article 5(3) does not require consent if cookies are used for technical purposes only, such as creating an authenticated session.

From the viewpoint of this thesis the most important part of article 5(3) is the definition of consent. When defining what constitutes as valid consent, article 5(3) of ePrivacy refers to directive 95/46/EC. Directive 95/46/EC is no longer in force, but it has been repealed by Regulation (EU) 2016/679 of the European Parliament and of the Council, also known as the General Data Protection Regulation (GDPR). As stated in GDPR article 94(2):

“References to the repealed Directive shall be construed as references to this Regulation. […]”

Therefore, our definition of consent is found in the GDPR. There are multiple articles that are used to define what consent is. Article 4(11) has the following description of “consent”:

“Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

In addition, recital 32 of the GDPR states among other things:

“Silence, pre-ticked boxes or inactivity should not therefore constitute consent.”

In addition, article 7(3) of the GDPR states:

“The data subject shall have the right to withdraw his or her consent at any time. […] It shall be as easy to withdraw as to give consent.”

The GDPR is important not only because it defines consent, but also because non-essential marketing and analysis cookies are often used to collect personal data. Personal data means any data that can be used to identify a specific individual. This definition originates from article 4(1):

“‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”

According to the GDPR processing personal data requires data subject’s consent, so the use of cookies usually requires consent for two reasons: storing the cookie on the user’s device requires consent, and using that cookie to identify that user also requires consent. As an interesting detail, recital 30 of the GDPR classifies internet protocol (IP) addresses as personal data, and thus processing of IP addresses cannot be done without data subject’s consent.

An interpretation of the ePrivacy directive and GDPR that is most likely incorrect is that one can set cookies on the end user’s terminal without obtaining consent if it is in the “legitimate interests” of the website operator. There is indeed a legitimate interest clause in recital 47 of the GDPR and it can under certain circumstances give the right to process personal data without the explicit consent of the data subject. However, directive 2009/136/EC or the Information Society Code have no mention of “legitimate interest”. Therefore, even if the website operator can indeed process personal data without obtaining consent, it does not give them permission to use cookies. Cookies can only be used when the user has consented to it.

These are the most important statements in the EU regulations and directives concerning consenting to cookies. According to GDPR, any consent that is obtained by violating one or more of the above principles is invalid.

As with all legal matters, how laws are interpreted in courts can be just as important as the laws themselves. In 2019 it was ruled that the company Planet49 had used an invalid method of obtaining cookie consent from people visiting a certain website under their control. The “Planet49 decision” affirmed that a pre-ticked checkbox does not constitute consent. The court ruled that the wording of the directives and regulations clearly denote that consenting is active, not passive behavior. This set an important precedent and confirmed that laws concerning the matter are valid. (Case C-673/17, 2019)

In 2020, France fined Google a total of 100 million euros for the use of cookies “without obtaining prior consent and without providing adequate information”, also confirming that the laws are indeed valid and can be enforced. Amazon faced a 35 million euro fine for the same reason. (CNIL, 2020a; CNIL, 2020b)

The European Data Protection Board has ruled that blocking access to a website if the user does not accept cookies (“cookie wall”) is illegal. (European Data Protection Board, 2020)

2.3. Cookie policies in Finland

In Finland marketers and privacy-minded people both have lived in confusing times. There are two government agencies that are responsible for enforcing the laws in question. To be specific, traditionally Data Protection Ombudsman's Office is responsible for enforcing GDPR and Finnish Transport and Communications Agency (Traficom) enforces Information Society Code §205. Traficom had insisted since the dawn of GDPR that user has consented to the use of cookies if they have not blocked cookies in browser settings. This statement had multiple issues, such as:

- As stated in chapter 2.2, pre-ticked boxes or inactivity should not constitute consent. Browsers, however, allow cookies by default.
- Blocking cookies with browser settings block all cookies, including those that are necessary from a technical standpoint. Blocking all cookies makes normal web browsing effectively impossible.
- Blocking cookies with browser settings only blocks actual cookies, not any related technologies even though the regulations apply to those technologies as well. For example, disabling cookies in browser settings does not block the use of tracking pixels, fonts or localStorage.
- It is in violation of the Planet49 decision described in chapter 2.2.

Even after these issues were pointed out to Traficom they continued to insist that browser settings can be used to signal consent (Tolvanen, 2021). Traficom continued to do so even after the Planet49 decision (Traficom, 2019). A ruling made later by the Deputy Data Protection Ombudsman that was in line with the European legislation had likewise no effect on Traficom's policies (Office of the Data Protection Ombudsman, 2020). At this point the two agencies were giving citizens directly contradicting instructions. Only after Traficom's interpretation of the Information Society Code & GDPR were challenged in the Administrative Court of Helsinki in 2021 and Traficom lost did they change their guidelines. (Decision H1515/2021, 2021; Traficom, 2021a)

The new instructions published by Traficom in September 2021 are in line with the regulations of the rest of the EU. The new guidelines for example explicitly ban cookie consent mechanisms in which declining to the use of cookies requires more clicks than accepting them. Using "legitimate interest" to justify cookie usage is likewise forbidden. (Traficom, 2021b)

Lax enforcement of the law also creates a problem. A website was reported to Traficom for possibly using cookies without consent. When Traficom

investigated, the website operator stated that they have removed all cookies from their website. Traficom dropped the investigation. (Decision H1515/2021, 2021) If website operators can avoid all consequences of illegal use of cookies by temporarily removing cookies for the duration of the investigation Finland is effectively not enforcing the law. It remains to be seen if this continues in the future.

To date, no organization has been fined in Finland for illegally using cookies (Tolvanen, 2021).

To summarize, in recent years Finland has interpreted the laws concerning cookies differently from the rest of the European Union. While the situation has now changed, it will most likely take some time before all websites are fully compliant with the new, more universal interpretation of mentioned laws and regulations. It is also uncertain how effectively the new regulations will be enforced.

2.4. Benefits of cookies for website operators

In order to better understand motivations behind cookie banner designs, it is important to understand why companies are using cookies in the first place and what kind of benefits the website operator receives when a visitor accepts cookies.

Simply put, website operators receive direct or indirect financial benefits and a competitive advantage if their visitors consent to the use of marketing and analysis cookies.

An example of indirect financial benefit is the ability to track visitors' movements when they browse a website. With a properly configured analytics service it is possible to see what pages users browse, for how long and when they leave a website. It is also possible to see when they drop off during a checkout process and record the mouse movements of a visitor (Hotjar, 2021; Google Analytics, 2021; Adobe Analytics, 2021; Matomo, 2021). There are other uses as well. The information obtained this way can be helpful both when identifying technical problems and when gradually improving the content on a website. In other words, tracking technologies help website operators to decide how to change their website to increase the percentage of visitors who decide to perform an action desired by the website operator such as making a purchase (conversion rate). The use of these technologies can give a significant competitive edge when compared to a company that does not have these tools at their disposal.

Direct financial benefits come in the form of advertisements. A website operator can join an *advertisement display network*, such as Google AdSense (2021). The website operator simply has to add a short code snippet to the website and their website starts showing ads to anyone who visits the website. The display network owner pays money for each advertisement shown to the visitor or clicked by a visitor (criteria may vary). The ads shown to the visitor vary based on what the ad display network provider knows about the visitor to maximize the click rate. Sometimes the expression “personalized ads” is used (figure 1).

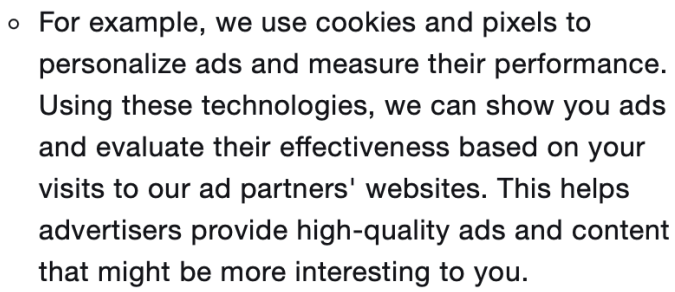


Figure 1. *Twitter states that they use cookies to personalize ads based on the user’s interests. (Twitter Help, 2021)*

There are also the ad display network providers themselves to consider. Companies such as Google LLC. and Meta Platforms, Inc. offer a variety of free services to users and web developers. Meta Platforms offers various social media services such as Facebook, Instagram and WhatsApp. Google LLC offers Google Search and YouTube, for example. These platforms let these companies to gather a significant amount of data on their users’ interests. The more data they collect, the more accurately they can predict the behavior of their users and the better they are at targeting ads at the users.

More interestingly Google, Meta and others can also collect data from people visiting websites that they do not own. They provide free services, such as Google Fonts and Google Analytics for developers to install on websites. Facebook has used its “like” button plugins to collect information about internet users (Acar et al, 2015). Every time a person with IP address X visits website Y that uses a web font from Google Fonts or a Google Analytics script, Google will know that website Y was visited by someone with IP address X. It is impossible for Google not to know it. That is simply how the Internet works. (Kaspersky, 2021; MDN Web Docs, 2021b) If the person with IP address X then visits to, say, YouTube can the IP address also be associated with a specific Google account. Due to indexing websites for their search engine, Google also

most likely has a general idea of what website Y is about and what kind of people generally visit it. In addition to IP addresses, there is usually other data transmitted in request headers that might allow for more precise identification of the individual, and with Javascript a near-unique combination of hardware and browser characteristics can be collected. This tracking method is known as fingerprinting (EFF, 2021).

An important use for cookies is known as remarketing. Let's say a user visits a website that sells motorcycle parts and that website has enabled remarketing through Google Ads. The website is using a Google Analytics script (figure 2) or a Google Ads script that can be used to identify the visitor. When the user leaves the website, he or she will see ads about the motorcycle parts sold on that website on other websites that are part of Google's ad display network. (Google Ads Help, 2021a)

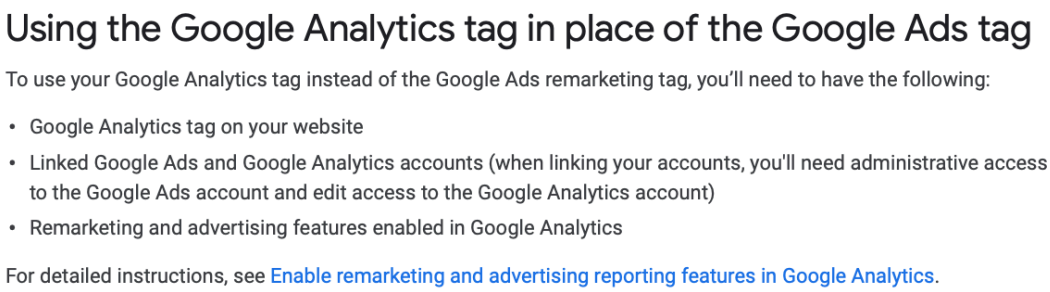


Figure 2. *Google Analytics can be used to target advertisements at website visitors (Google Ads Help, 2021b).*

Just because these service providers *can* combine data from website visits with data from their own services does not mean that they *do*. However, it is unclear why Google and others would offer these free services if they did not benefit from them. It is perfectly possible that the IP addresses obtained from pixels, fonts and Javascript snippets are used for nothing and they are either obfuscated or never stored anywhere at all. Still, it is theoretically possible to store and process the data, there is a financial incentive to do so and since the technology is proprietary it is impossible for outsiders to be sure either way. According to the GDPR an organization must be able to prove that it acts in accordance with the GDPR, which makes this last statement problematic.

It is unclear how many websites exactly use these services, but according to estimates the just the mentioned Google Analytics is used on approximately 29 million websites (Built With, 2021a). Google Fonts is used on approximately 43 million websites (Built With, 2021b). There could be hundreds of millions of websites equipped with third-party technologies that are used for tracking

purposes. This raises an interesting question: how aware are website operators of the fact that they are sharing data visitor data with third parties? For example, Google and Meta market their analytics and display ads services as things that are easy to set up: the user only needs to add one code snippet to their website for the service to work (figures 3 and 4; Facebook for Developers, 2021). Needless to say, having the skill to copy and paste does not guarantee understanding of cookies or web tracking. This is important when we consider alternative, more privacy-friendly solutions for web analytics: some website operators who use third-party solutions might consider moving to more privacy-friendly and cookieless analytics options such as monitoring server logs if they were more knowledgeable about cookies and third-party data collection.

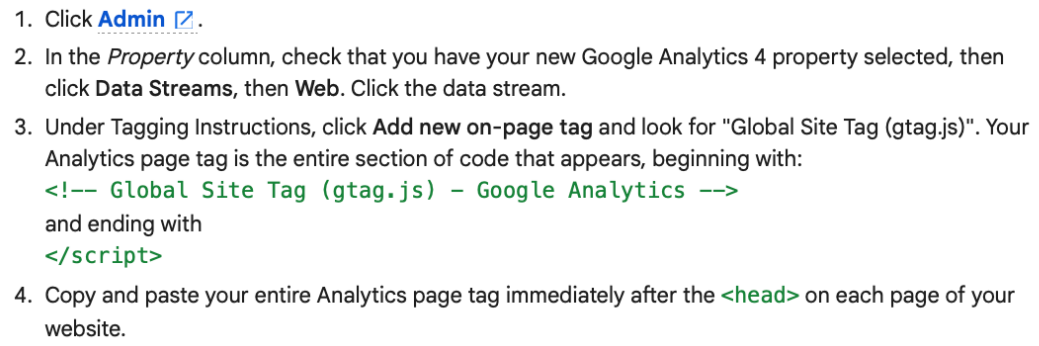


Figure 3. *Google markets its Analytics as a service that can be installed by copying and pasting one code snippet to the website source code. No knowledge of cookies is required. (Google Analytics Help, 2021)*

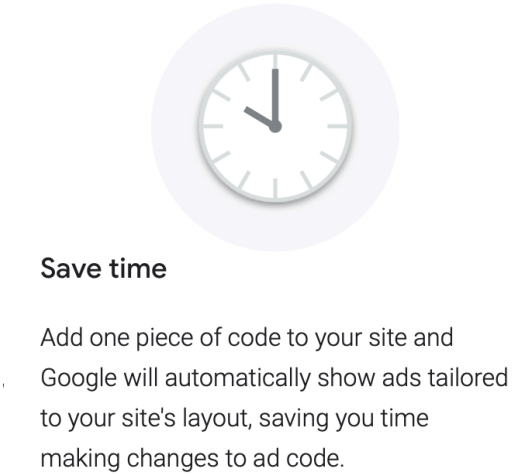


Figure 4. *Google also markets its AdSense as a service that works by just adding one line of code to the website. (Google AdSense, 2021)*

Technologies such as ad display networks and sophisticated website analytics cannot function without storing some data on the end user's terminal. Therefore, there are powerful economic incentives for companies to get as many people as possible to consent to the use of cookies.

2.5. Benefits of cookies for website visitors

While it can be established beyond doubt that cookies and related technologies are extremely beneficial for marketers and website operators, are they beneficial for consumers as well? This is more difficult to prove.

Since one of the most important uses for cookies is targeted advertising, let's start with that. It could be argued that it is in the interests of a consumer to receive advertisements of products they are likely interested in. It is likely true that there are people who enjoy seeing ads that are relevant to their interests, at least when compared to seeing ads that are not relevant to their interests. In a study by Melicher et al. (2015), it was discovered that 74% of the participants liked seeing more relevant advertisements compared to less relevant ones, but 60% found targeted advertisements harmful in at least one scenario that was presented to them.

Many websites and services are funded by targeted advertising. Facebook, for example, had 1,84 billion daily active users in 2020. During that time Facebook's ad revenue was 85,965 billion US dollars. From this we can make the estimate that each user brings Facebook 3,89 dollars per month (2,56 dollars if we also count those logging in at least once a month) (Facebook Investor Relations, 2021). Without targeted ads, this revenue would have to come from somewhere else. One option is that users would pay money for a subscription. Therefore it could be argued that personalized ads are beneficial for consumers because they make certain free services possible.

The ads could also theoretically function without tracking technologies and therefore be no more personalized than those seen on television, for example. After GDPR, The New York Times gave up using targeted advertising in Europe. This has not affected their ad revenue negatively. (Davies, 2019) This signifies that there is at least one case in which users were able obtain the same benefit (access to the service) without data collection.

There are other possible, less privacy-intrusive sources for income as well. Brave web browser has a built-in mechanism for showing ads without identifying the users. Advertisement income can also be shared with content creators. (Brave Ads, 2021)

An important use for cookies is improving the usability of web services. With the help of tracking technologies it is easy and cost-effective to create recordings of real-life users using a service and thus identify pain points and technical problems. Users subsequently benefit from the improved service. There are other ways to perform this type of testing, though. Test candidates could be recruited for a usability study conducted in a user experience laboratory. This is, however, more time-consuming than simply installing a script on a website. Laboratory testing therefore requires more dedication and resources than using an online tool.

2.6. Reasons for refusing cookies

Despite the possible benefits listed above, many people choose to not accept cookies (Van Bavel & Rodríguez-Priego, 2016; Bauer et al., 2021). The reasons for doing so are easy to understand. Article 12 of the Universal Declaration of Human Rights starts with the phrase “No one shall be subjected to arbitrary interference with his privacy”. Privacy is a fundamental human right which indicates that it is considered to be inherently valuable.

There are also tangible consequences to losing one’s privacy. Let’s assume for a second that a person accepts cookies on every site he or she visits. As a consequence, the data from every page visit that person makes is transferred to a data broker, an entity who makes money by collecting personal data and selling or licensing it to interested parties, usually for marketing purposes (Gartner, 2021; Avast, 2021). For example, there is a data broker known as Acxiom that according to Singer (2012) claimed to have data about 500 million consumers worldwide in 2012. The data collected can be incredibly detailed, including everything from how many seconds a certain page was looked at to recorded mouse movements. It may also be possible to combine this data with information scraped from other sources such as social media profiles. Provided that it is legal, some stores and other institutions are also willing to sell for example purchase information to the data brokers, providing even more sources of information that can be combined with browsing history (WebFX, 2020).

Now, let’s assume that all this information is either sold to a malevolent entity or leaked as a part of a security breach. In a worst-case scenario, what can personal data be used for? Browsing data may reveal sensitive information such as health information, sexual preferences or political views. In the Cambridge Analytica scandal data collected from Facebook profiles was used to create precisely targeted political advertisements in order to alter voting behavior (Hern, 2018). Dating app Grindr has leaked information on sexual

orientation and HIV status to third parties (Forbrukerrådet, 2018a). In the wrong hands, this is data that could potentially be used for blackmail or ransoming.

To provide a somewhat less extreme example, there is price discrimination or “personalized pricing” as the proponents call it. This refers to using personal data to determine how much a person is willing to pay for a product or service and then pricing the items accordingly. According to Zuiderveen Borgesius et al. (2017) such pricing methods might even be illegal according to Article 22 of the GDPR. Be that as it may, for example Tinder prices its premium subscriptions differently based on your age, gender, sexual orientation (these are obviously provided by users) and a number of unknown other factors where the source data is unknown (Jeong, 2020). Several tourism/hotel related websites also seem to use some form of personalized pricing (Hindermann, 2018).

In general, the more information you have about a person the easier it is to predict and thus influence their behavior. If the information is sensitive, the person can potentially even be coerced to take certain actions by threatening to make the information publicly available.

In conclusion, there can be very serious consequences to rampant data collection. This means that there can be a conflict of interests between website visitors and website operators.

3. THEORETICAL FRAMEWORK

This chapter is about human decision-making, its caveats and how it can be influenced and exploited by those who wish for a person to take an action that is not in his/her best interests. This chapter also briefly explores the findings of other studies concerning human interaction with cookie banners.

For this chapter, a literature review was conducted by searching for information on Scopus. All English publications containing “consent pop-up”, “consent notice”, “cookie banner” or “cookie pop-up” in title, abstract, or keywords were included in the search. To obtain the latest data concerning the subject the results were limited to year 2019 or newer. The timespan was found to be especially important since it is likely that people react differently to cookie banners after seeing thousands of them when compared to the situation right after GDPR when banners were a new phenomenon. This resulted in 185 results. The list of results was then reviewed manually. 176 articles had a title or abstract that immediately revealed that it was either not relevant to the field of ICT and human-technology interaction or they were about something else than researching interaction with cookie banners. Those were discarded and the remaining nine articles were then read and the findings included to this chapter, if there were any.

Chapters 3.1. and 3.2. present three psychological theories which may be used to explain behavior when facing a cookie banner. Chapter 3.3. explains the definition of a “dark pattern”, a category of design patterns often found in cookie banners and the theory behind it. Chapter 3.4. focuses on the reasons people give when asked about their interaction with banners. Finally, chapter 3.5. discusses the biases people might have when dealing with both cookie banners and privacy matters in general. 3.6. is a summary of the findings.

Table 1: cognitive systems

Automatic	**Reflective**
Uncontrolled	Controlled
Effortless	Effortful
Associative	Deductive
Fast	Slow
Unconscious	Self-aware
Skilled	Rule-following

3.1. Cognitive appraisal theory and protection motivation theory

The cognitive appraisal theory states that any emotion that follows an event is not caused by the event itself, but the person's perception of that event. After an event occurs, *primary appraisal* takes place. It is a cognitive process which is used to interpret the event as either positive, dangerous or irrelevant. After this, *secondary appraisal* occurs. During the secondary appraisal a person analyzes their ability to handle the situation. If resources are found to be insufficient, a stress reaction occurs. (Lazarus & Folkman, 1984)

The protection motivation theory (PMT) is originally based on the cognitive appraisal theory. According to this theory when appraising a threat people assess its perceived severity and likelihood. Then coping appraisal occurs, and people will assess if they have effective means for removing the threat (response efficacy) and their perceived self-confidence for successfully executing these actions (self-efficacy). If they believe that they have insufficient means of coping with the threat the response will be maladaptive, such as denial or ignoring the threat entirely. (Rogers, 1975 & 1983)

If we now assume that people consider cookie banners a privacy threat (which is by no means certain), we can use this theory to try to explain their behavior. There are three outcomes to consider: If the users appraise the banner as something irrelevant, they would most likely take the action that is the quickest at removing it from sight. If the users consider themselves to have the ability and self-efficacy to execute the actions to remove the threat, they would decline cookies, thus removing the privacy threat. If the user feels like they don't have the ability or self-efficacy to remove the threat, there is a maladaptive response. In this case the large number of banners might be a cause for the low self-efficacy: if the user perceives that in the bigger picture there is nothing they can do to stop online tracking, they might ignore the threat.

The protection motivation theory is referenced in an early cookie banner experiment by Van Bavel and Rodríguez-Priego (2016).

3.2. Dual process theory

According to Chaiken and Trope (1999) people essentially have two cognitive systems for decision-making. We can call them Automatic and Reflective. In the 2008 book *Nudge: Improving Decisions About Health, Wealth, and*

Happiness by Thaler and Sunstein describe the properties of the two decision-making systems. They are shown in table 1.

Simply put, the automatic system is something we would call intuition and the reflective system is more thorough reasoning. Usually, big life choices such as choosing a career are handled by the reflective system, whereas simple things such as choosing a gear while driving or which way to steer is handled by the automatic system (at least for experienced drivers).

In his 2011 book *Thinking, Fast and Slow* David Kahneman refers to similar constructs by the names System 1 and System 2. He gives several examples of activities utilizing one of the two systems. System 1 is used in occasions such as driving a car on empty roads, completing the phrase “bread and…”, answering to what is 2 + 2 and detecting if one object is more distant than another. On the other hand, System 2 is utilized for example when counting the occurences of the letter A in a page of text, looking for a woman with white hair, focusing on the voice of a particular person in a crowded and noisy room, filling out a tax form or checking the validity of a complex logical argument.

Chabris and Simons give a well-known example of the human use of these two systems in the 2010 book *The Invisible Gorilla*. A short film of basketball players is presented to the test participants and they are told to count the passes made by one of the teams. Halfway through the video, a person in a gorilla suit walks to the basketball court, thumps their chest and then walks away. About half of the participants completely fail to notice the gorilla, as counting the passes requires allocating every bit of a person’s attention to System 2. A person without a complex task such as counting the passes would easily spot the gorilla using their System 1.

References to this decision-making model are frequently found in related literature (Bauer et al., 2021; Utz et al., 2019; Nouwens et al, 2020; Mathur et al., 2019; Van Bavel & Rodríguez-Priego, 2016; Soe et al., 2020).

3.3. Nudge theory and dark patterns

First, let us define what exactly is a nudge. We can again rely on Thaler and Sunstein’s (2008) book about nudges. The book defines nudges as follows:

“A nudge, as we will use the term, is any aspect of the choice architecture that alters people’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not.”

There are numerous examples of the successful application of the nudge theory. For example, the famous men's urinals of Schipol airports have housefly etches. Men instinctively aim for the houseflies, which has resulted in a 80% reduction in spillage. This is also why it is effective to place snacks right next to the counters in stores. A speed sign that notifies drivers about their current speed is also an example of a nudge. (Mauricio Mejía, 2021) None of these examples force the person being "nudged" to change their behavior in any way as described in the definition, yet the behavior changes anyway.

Why do nudges work, then? Summarized, the idea behind nudge theory is that the automatic decision system is quite susceptible to external influences. Simply by presenting the choices to the user in a certain way we can significantly impact the choices the user's automatic system makes. To provide yet another example of this, Google once tested 41 shades of blue for the links in Google Ads to see which one people were most likely to click. A former Google executive claims that choosing the optimal shade of blue for the links influenced the user's decisions so much that it boosted the ad revenue by 200 million dollars per year (Holson, 2009; Hern, 2014). One can also try to design the choices so that a person will be likely to use the automatic system instead of the reflective one when making the choice.

In their book Thaler and Sunstein (2008) focus mostly on examples of using nudges to help people accomplish things that are in their best interests, such as choosing healthier food in a grocery store. However, nudges can just as easily be used to manipulate people to making choices that might not be in their best interests. In user interface design, these types of nudges are called dark patterns. Chris Nodder, author of the 2013 book *Evil by design* defines "evil design" (essentially dark patterns) as follows:

"…evil design is that which creates purposefully designed interfaces that make users emotionally involved in doing something that benefits the designer more than them."

The definition differs slightly between sources. "Dark pattern" can also be used to refer to interfaces in which avoiding the option that benefits the designer more than the user is almost impossible and therefore per Thaler and Sunstein's (2008) definition does not count as a nudge. (Brignull, 2021; Forbrukerrådet, 2018b; Maier & Harr, 2020). In any event, whenever the expression "dark pattern" is used in this thesis the reader may assume it is used to refer to a specific kind of a nudge.

Despite the ethical issues dark patterns are commonly found on websites due to the fact that they perform well in A/B testing and using them leads to better

sales and conversion. Financial incentives make utilizing them desirable, at least on short term. (Brignull, 2011; Keith, 2017)

Dark patterns are frequently found in cookie banners. A study by Soe et al., (2020) in which 300 cookie banners were manually reviewed discovered that all of the reviewed websites used a dark pattern of some kind. The websites included in this study were Scandinavian and English-language news outlets websites and magazine websites. 297 of the 300 websites had an option to deny consent. However, denying consent with a single click was only possible on 15 websites whereas agreeing with one click was possible on all of the reviewed websites. A study by Nouwens et al. (2020) that consisted of scraping 10 000 top UK websites for CMP's resulted in a similar discovery, stating that of the websites that were using a CMP all websites had an "accept all" button but only 12.6% had a "reject all" button that was accessible without additional clicks.

In an experiment by Bauer et al. (2021) conducted on a Danish B2B website in 2019 it was discovered that by implementing small changes in the appearance of the accept/reject buttons of a cookie banner it was possible to significantly alter the chance of a visitor consenting to the use of cookies. In the control experiment a banner with equally prominent "accept" and "reject" buttons were provided for the user. In the test banned used for comparison adding text, positively framing the use of cookies, hiding the reject link among the text and highlighting the accept-button in green resulted in an 85% increase in the amount of consents, meaning that an additional 17% of website visitors agreed to the use of cookies.

3.4. Privacy behavior

While there is research to be found on how design changes affect the consent rate on websites, few of the articles that were found for this literature review strive to explain people's behavior with anything but psychological theories (as opposed to asking them about the decisions they made or determining if they would have made the same choices under different circumstances). There is, however, other research on the matter of privacy behavior such as the very comprehensive literature review by Gerber et al. (2018).

It is very important to note that survey results clearly reveal that people worldwide consider online privacy to be important. It is equally important to note that in practice these same people do very little to protect their privacy. (Gerber et al. 2018) This is sometimes called "the privacy paradox" and it is something to keep in mind when considering the effect of nudges and dark

patterns. Nudges are likely to be a very powerful force on the field of privacy options due to this apparent indifference towards privacy-enhancing actions. It is also something to consider when analyzing the results of any experiment about cookie banners. Answers to questions such as “what would you do in scenario x” might not give any indication of behavior in the real world.

Considering the gap between privacy attitudes and privacy behavior, we have to assume that there is a high likelihood for a phenomenon known as cognitive dissonance. According to Festinger (1957) when two cognitions or actions are inconsistent with each other, it results in a dissonant relationship with reality. To provide an example, the belief that privacy is important is incompatible with the action of ignoring privacy policies. Cognitive dissonance causes discomfort which, if significant enough, causes people to seek consistency between their actions and beliefs. In this case this might happen through justification on one’s actions by adding new information to the cognition which is known as rationalization. Rationalization is more broadly defined as finding seemingly logical reasons to justify one’s actions, especially those that are either socially unacceptable or made for no known reason at all (Cambridge Dictionary, 2021; APA Dictionary of Psychology, 2021). Therefore, a person might explain their inconsistent privacy behavior with reasons such as “My personal information is spread across the internet anyway”, “I was in a hurry” or “Doesn’t everyone skip reading these disclaimers?”.

The privacy paradox can be demonstrated for example with a study by Utz et al. (2019). Only about 0.1% of visitors accepted cookies from all categories when they were presented with multiple cookie categories and empty checkboxes for selecting them. When the checkboxes were full, 83.5% accepted all categories demonstrating that in privacy matters people are likely to choose the default option, whatever it is. The study also demonstrates the power of nudging using default options.

Privacy choices are sometimes explained using a “privacy calculus” model (Xu et al., 2008). In this model people are expected to weigh the possible options and then make a decision based on the benefits of accessing the service and risks and costs of a possibly privacy infringement. If the benefits seem to be greater than costs, they agree to data processing. According to Gerber et al. (2018) data supports this model, at least to some extent. However, it is unlikely to be a good predictor of behavior in this case. Graßl et al. (2021) discovered that 40% of their research participants didn’t read cookie notices, and another 48.2% admitted to only skimming them. If a person does not know what they are consenting to, they can’t possibly assess the benefits and costs of the

consent. In that case their behavior might either be based on assumptions of what they are consenting to or they might ignore the privacy cost entirely.

There is also evidence that if a banner provides more feeling of control or power to the users, people are more likely to accept cookies or using the collected data collection for various purposes (Bornschein et al. 2020; Schmidt et al. 2020). One way to increase the perception of control is to present the user numerous options in privacy settings and provide a comprehensive description of how their data is used. The protection motivation theory can explain this behavior, at least to some extent. When a person is feeling that they are threatened or in this case their privacy is threatened, their coping appraisal would be more likely to appraise the threat as manageable if the person feels they can do more about it. Therefore if the user is presented with a control panel, they can happily ignore it as demonstrated by Graßl et al. (2021) when they discovered that hiding the decline-button behind a button labelled “Manage options” increased the perception of control (and the amount of consents).

Kulyk et al. (2018) discovered four important properties that affected how likely people are to stay at a website when facing a cookie banner. These are: the importance of the content of the website, the perceived trustworthiness of a website, sensitivity of the data that is collected by the website either through the use of cookies or if the user is meant to input sensitive data on the website itself. Finally, familiarity with the website can also be a factor based on which they accept or reject cookies. The trust factor is also mentioned by Gerber et al. (2018) in their paper. However, at this point it is necessary to remind the reader of the privacy paradox: just because a person states in a questionnaire that they would leave a website under some circumstances does not mean that they would actually take such action.

Utz et al. (2019) conducted an experiment on a German eCommerce website in which test participants were asked to explain their choices they made after interacting with the banner. When asked what they thought would happen if they declined cookies, most participants were under the impression that they would be blocked from the website or parts of the website would not work if they refused cookies. Many also expressed concern that the choice they made would not, in fact, make any difference. When asked what they thought would happen if they accepted cookies, many answered that their personal data would be processed. Some focused on describing what a cookie is, and many stated that they can continue using the site if they accept cookies.

3.5. Decision biases

There are various decision biases that can be used to explain the discrepancy between privacy attitudes and privacy behavior. Some of them are also likely to influence the results of the empirical research conducted for thesis. The ones considered to be most relevant for the subject at hand are listed here.

- The optimism bias: people tend believe that they are less likely to experience negative events compared to other people (Thaler & Sunstein, 2008). For examples of possible negative events, see chapter 2.6.

- The availability bias: When asked what is the likelihood of an event most people tend to answer based on what sort of examples come to mind (Kahneman, 2011; Thaler & Sunstein, 2008). Considering the stealthy nature of data collection determining even the causal relationship between data collection and consequences (which could serve as examples of negative events) can be difficult or even impossible. For example, a person can be subjected to price discrimination without them even knowing it: it is not possible for a website visitor to determine why they see the prices they see unless the website reveals that information on purpose. Facebook is also known for purposefully undermining efforts to understand why a person sees the kind of ads they see (Signal, 2021; Vincent, 2021; Brandom, 2021). Since personal data can be collected from so many sources it can be impossible to determine that the decision to accept cookies on a certain website or on multiple websites has led to negative consequences.

- The immediate gratification bias: People tend to prefer immediate benefits to future benefits (Thaler & Sunstein, 2008). Accepting cookies provides the immediate benefit of accessing a website whereas the benefits of protecting one's privacy and personal data take place in the future.

- Rational ignorance: refraining from acquiring knowledge when the perceived cost of learning about an issue is higher than the expected potential benefit that the knowledge would provide. In this case, the perceived costs of learning how data is used could be higher than expected benefits of simply ignoring the costs and sharing the data. (Downs, 1957)

3.6. Summary

According to the nudge theory, even near-insignificant changes in user interface design can have an impact on user behavior. Defaults are especially powerful as demonstrated by Utz et al. (2019). The color and size of buttons was also found to be effective by Bauer et al. (2021).

The applicability of many other research results depend on how much attention people pay to cookie banners. The applicability of the privacy calculus model or protection motivation theory is dependent on how carefully people assess the privacy threat, and as Graßl et al. (2021) discovered people do not seem to pay much attention to cookie banner texts, indicating they won't be able to make an informed decision concerning the matter. The privacy paradox also indicates that research that only measures privacy intent is not likely to accurately predict privacy behavior. Nevertheless, if we assume that the privacy intent research conducted by Kulyk et al. (2018) signifies that the perceived trustwrothiness of a website has at least some effect on behavior, the result is important considering this thesis. In the experimental stage the participants are told they are participating in research which will possibly have an effect on the research results. Various decision biases and cognitive dissonance might also affect behavior.

4. RESEARCH QUESTIONS AND PROCESS

This chapter concludes the literature review phase. Chapter 4.1. forms the outline for the research questions while chapter 4.2. introduces a broad overview on how the three-part study was conducted.

4.1. Establishing the research questions

The most important objective for this thesis is to discover what kind of choices people make when facing a cookie banner and what is the reasoning behind their decisions. This information will, in turn, suggest that a consent obtained through the use of a cookie banner is either valid or invalid. If it can be proven that website visitors generally base their decision to accept cookies on mostly other things than what they are actually consenting to, it can be interpreted to mean the visitors have not made an informed decision. This is a very broadly defined topic, however. For this reason three more specific research questions were created. The first one provides the necessary information to answer the second and third while hopefully also providing interesting data on its own.

In order to provide a realistic test environment for the users it is first necessary to research what kind of cookie consent mechanisms they are likely to see in everyday life. This brings us to our first research question:

RQ1: “What kind of cookie consent banners and mechanisms are in use on Finnish websites?”

Once research question 1 is answered, it is possible to design and then implement realistic test cookie banners for testing the remaining two research questions.

RQ2: “How does the amount and purpose of information collected using cookies affect probability of consenting compared to design changes?“

a) **How does changing the color of the buttons affect consent rate?**

b) **How does arrangement of the buttons affect consent rates?**

c) **How does the amount and purpose of the information collected affect consent rates?**

This question was chosen based on the assumption that cookie banners can have two significant properties that can influence the decision made by a website visitor when facing a cookie banner:

1) the content of the cookie banner, including information such as what cookies are used, how much personal data is collected and how it will be processed etc. This kind of information would most likely be processed by the reflective decision-making system.

2) the design of cookie banner; its layout and colors, what buttons and links are present, how they are labelled and the contrast and size of the various elements in the banner. Small changes in design would most likely have an effect on the automatic decision-making system.

In theory, one should be able to form a relatively good picture of what kind of decisions are made and why by creating variations of both properties, presenting them to the users and recording how users interact with the banners. However, it is very important to note that the original assumption based on which these research questions were chosen turned out to be profoundly incomplete. More of this in results and discussion sections of chapter 7.

RQ3: “Besides content and design, are there other significant factors in cookie banners that influence user behavior?“

In addition to simply answering these questions, the thesis will also aim to find out why the results are what they are and promote understanding on why people choose one option over another when facing a cookie banner.

Once the study is complete, the results will in the best case result in better laws and regulations concerning online tracking and the use of cookies. It is in the hopes of the author that it will help to end the era of consent fatigue.

4.2. An overview of the research process

In order to answer the selected research questions, an empirical research process with multiple stages was conducted. The empirical work in this thesis is divided into three stages.

The first stage focuses on preliminary review of cookie banners on popular Finnish websites. In practice, this phase involved visiting a number of websites that are popular in Finland, taking screenshots of any cookie banners that are present and then going through the results with the aim of discovering any

common elements that are present in the said banners. With this information, stage one answers the first research question and acts as the basis for the following stages.

The second stage includes the design process for the test cookie banners based on the design constraints discovered in the first stage. It also describes how the test website was created and the implementation of the banners.

The third and final stage consists of a detailed description of the research process to answer the remaining two research questions, including the design of the user flow for research participants, the contents of the questionnaires used in the research process and how the research participants were recruited. This stage also includes discussion of the results.

5. STAGE 1: WEBSITE REVIEW

In order to create plausible cookie consent banner designs for users to test, it was necessary to first find out what kind of banner designs are currently in existence. Chapter 5.1. covers the research methods, chapter 5.2. focuses on the results of the review, chapter 5.3. contains analysis of the elements of these banners and chapter 5.4. covers further analysis of the results of the review.

5.1. Research method

A total of 50 Finnish websites were visited to obtain more information about what kind of designs were used to obtain consent from users. The funding and monetization of websites varies significantly across different industries. For example, a large multinational company manufacturing elevators does not need its website to display ads, whereas ads can be the only source for income for a news website. While the elevator manufacturer can benefit from the use of cookies as described in chapter 2, they are not as important as in the case of the news website. For this reason the websites included in the review were the chosen using the following criteria:

- Ten largest companies in Finland by market cap (Aunola, 2020).
- Ten largest eCommerce websites by revenue with main country set as Finland in Statista ecommerceDB (2021).
- Ten largest media websites according to Media Metrics Finland (2021).
- All Finnish websites in the Top 50 Websites Ranking by Similarweb (2021). The website was judged to be Finnish if it was both available in the Finnish language and aimed mostly at a Finnish audience. This excludes for example Google, Facebook and Twitch since they were judged to have an international audience.
- To reach the goal of 50 websites, four advertising agency websites were reviewed. Since advertising agencies are often responsible for both creating corporate websites and installing analytics and advertising functionality on them, their role in the field can be considered to be very influential. For this reason they were considered to be a natural addition to this thesis. No advertising agencies were included in any of the previously mentioned rankings.

The websites were visited using Mozilla Firefox web browser and screenshots were taken of all cookie banners. In addition to paying attention to the design elements of these banners, the amount of characters in the body text in each banner was measured. Special attention was also given to the contrast ratios of determine if poor contrast ratio was used to guide visitors to picking more privacy-friendly choices. The contrast rating was classified as FAIL, AA or AAA based on the Web Content Accessibility Guidelines (WCAG) (W3C, 2018). No other accessibility tests were conducted. If there was no banner, web inspector was used to determine if the website was using cookies anyway. Other than that it was not tested whether or not these websites actually respected the visitor's choices regarding cookies.

For a complete list of websites reviewed, see Appendix A.

5.2. Results for answering research question 1

The website review took place in May of 2021. All of the websites used were using cookies of some sort. 47 of the 50 websites reviewed also had a cookie banner.

5.2.1. Banner types

The cookie banners used on all of the reviewed websites fall into three main categories. These are defined as follows:

- Implicit grant: The website simply announces the user that they are using cookies or by using the website the visitor agrees to the use of cookies. There is no possibility to opt out (figure 5).

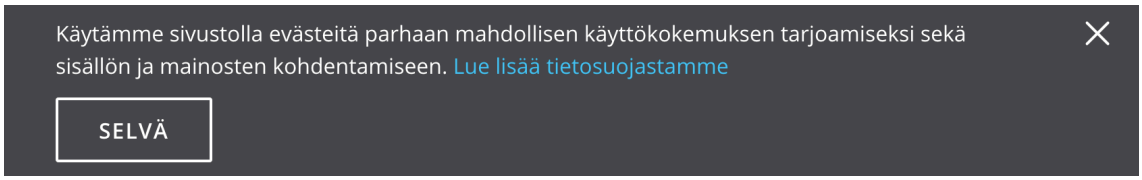


Figure 5. *Example of a cookie banner with implicit grant. There is no button for rejecting cookies: the banner can be closed by clicking the cross on the top right corner or the big button labeled OK.*

- Refusal hidden: The website shows a banner with two options: "accept all" and "settings". There is an option to refuse cookies but it is buried somewhere in the settings. Rejecting cookies is more difficult than accepting them (figure 6).

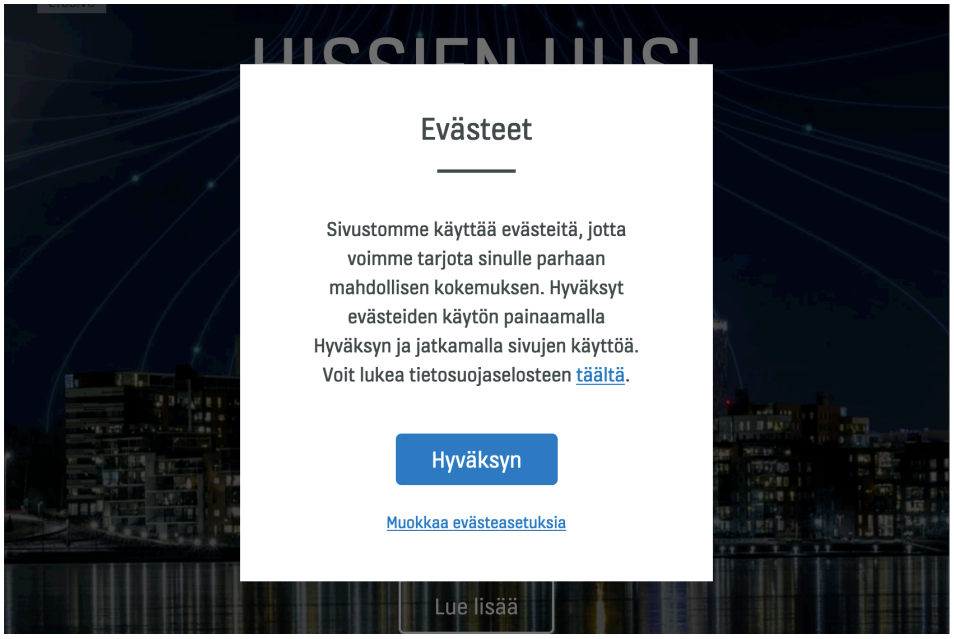


Figure 6. *Example of a cookie banner with the refusal option hidden. On the bottom note the big highlighted "I accept"-button and under it a smaller button with text "Change cookie preferences".*

- Neutral banner: The banner has a readily available option for rejecting all cookies that are not strictly necessary (figure 7).

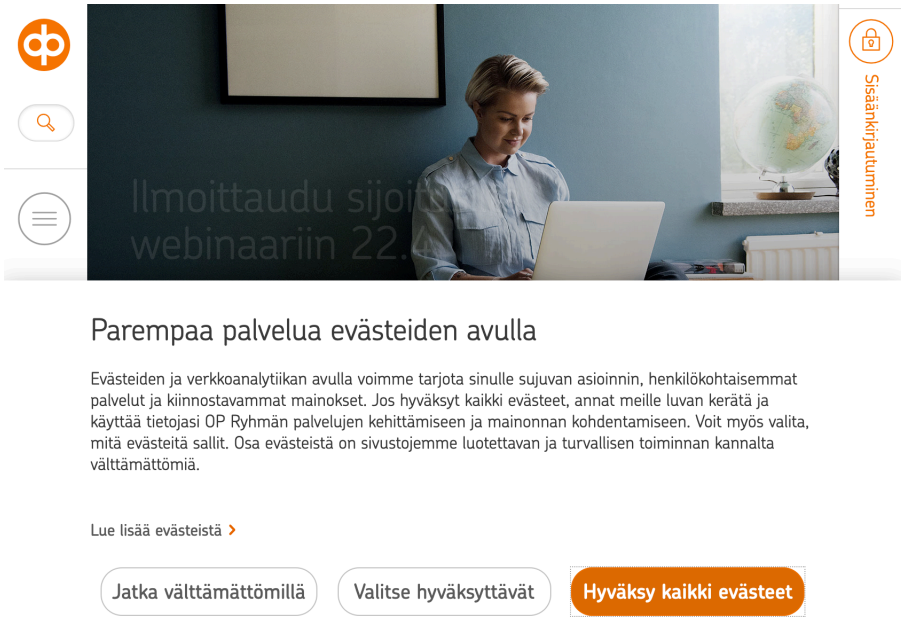


Figure 7. *Example of a neutral cookie banner. From left to right the buttons are: "Continue with necessary [cookies]", "Choose which to accept" and "Accept all cookies".*

5.2.2. Banner prevalence by type

Out of the fifty websites reviewed, seven had an *implicit grant* banner and six had a *neutral banner*. 34 websites had a *refusal hidden*-type banner.

Implicit grant and *refusal hidden* banners do not seem to comply with the regulations discussed in chapter 2.2. Despite this, the use of these banner types seems to be extremely common. This is possibly at least partially due to how Finland has interpreted the laws and regulations as discussed in chapter 2.

5.2.3. Common elements of banners

The reviewed *refusal hidden* and *neutral* banner types most commonly had the following elements:

- Darkened overlay that prevents the use of the website until the visitor has declined or accepted to the use of cookies. The banner itself appears on top of this overlay.
- Website or company logo.
- Headline stating that website uses cookies. Sometimes the headline was a bit more eloquent, such as “You decide how your personal data is used” or “We respect your privacy”. These are dark patterns, since telling users that they are in control tends to cause them to be less mindful about privacy settings.
- Text that is usually used to describe what the cookies are used for, but not in any great detail. More of this in the next chapter.
- A link to a privacy policy.
- Two or three buttons: type 2 banners have one for managing settings and one for accepting all cookies. Type 3 banners additionally have a button for refusing all cookies. The button for accepting all cookies was, with a few exceptions, large and had a brightly colored background. Most commonly used colors were blue, green, or whatever the main brand color of the website operator was. If the buttons were placed next to each other on the banner, the button for accepting all cookies was usually placed on the right side. The significance of this is unclear, but since website operators wish to maximize the consent rate this is hardly a coincidence. The button for accepting cookies generally is usually labeled as “I agree”, “accept all” or simply “OK” whereas the button for rejecting cookies is commonly labeled

"accept only necessary cookies" or "reject all". The button for going to settings is commonly labeled as "more settings", "cookie settings", "manage your settings", "settings" or even "show purposes".

- The settings page generally has the option to enable and disable various cookie categories such as marketing and analytics, as well as buttons for saving choices and accepting all cookies.

5.2.4. Length and content of body text

The body text length in these banners vary greatly. The shortest text found was merely 105 characters long, whereas the longest text was 1356 characters. The average length of text in banners classified as *neutral* or *refusal hidden* was 585 characters. Implicit grant banners were not included in this comparison since they usually had shorter texts and in the case of an implicit banner the consumer would not be able to make any decisions based on the contents of the texts.

The contents are for the most part similar. The website announces that it is using cookies. Some information about what the cookies are used for is also present, but this information tends to be rather vague. Most of the websites state that cookies are used for statistical purposes and improving the user experience of the website. The websites do not, for the most part, clarify how exactly storing information on the user's computer helps them to improve the user experience of the website or what kind of statistical information is collected or how accurate it is. The websites also announce that data is shared with "partners" or "affiliates" or "services offered by third parties". This most likely refers to the ad display network providers, but this is not clarified at any point. Either marketing or personalized content and advertising are also often mentioned in the texts. If the user chooses to click the button for more information, it is possible that they receive a slightly more detailed explanation on what cookies are used for.

It is worth pointing out that none of the banners mention any potential downsides for accepting cookies. According to the cookie policies on these websites, they quite often share data gathered from visitors with dozens or even hundreds of "partners". This was never mentioned on the first page in the text that was presented to the user, the information was only available on the settings page. The users were also not informed the possibility of this information leaking to outsiders. Likewise, it was not mentioned that the most important motive behind collecting this data is to alter the behavior of the user browsing the website as discussed in chapters 2.5. and 2.6.

5.3. Discussion

First, it is worth pointing out that all websites included in the review were using cookies of some kind, even those that did not have a banner. It was quite easy to place the banners into one of the three categories as there was little deviation between them. None of the websites prevented the user from accessing it with a cookie wall.

Some of the websites used a shared banner. For example, news websites that belong to Sanoma Corporation all use the same banner with the Sanoma logo. It was also fairly common to see third-party banner solutions, that is, CMPs. This can be a cost-effective solution since a website can have dozens of tracking scripts. It can be somewhat time-consuming to create a customized cookie banner that successfully disables all of those scripts and then successfully activates them if the user agrees to the use of cookies.

With a few exceptions, all of the websites used dark patterns of some kind to present accepting cookies a better option than rejecting them. On almost every reviewed website the button for accepting cookies was significantly larger and more brightly coloured than the button for rejecting cookies or going to a preference page to present it as the default option.

It is unclear whether or not the average website visitor can understand the link between storing information on their computer and improving the user experience on their website.

Only 17% of the banners complied with WCAG guidelines concerning contrast. Contrary to expectations, in most cases the button for going into settings or declining cookies was rarely the reason for failing this evaluation. More often the issues with contrast were caused by privacy policy links, buttons signifying acceptance and especially the toggle buttons that were used to adjust preferences in cookie settings. Judging by these results, it would not seem that there is any widespread and systematic misuse of contrast to outright hide undesirable choices from users; the designers behind these banners simply appear to be incompetent.

6. STAGE 2: CREATING A TEST ENVIRONMENT

Based on the results of the website review in chapter 5, four test banner designs were created. In order to make the banners appear natural, the most commonly appearing design elements in neutral banners were incorporated into test banners. Since implicit grant banners had no option to opt out, they were not analyzed further.

Initially, one of the designs was decided to be a common *refusal hidden* type banner in which it is not possible to decline cookies with one click. This was later dropped from the possible options and it was decided to focus on more subtle changes in design: hiding the option to decline cookies is likely to be illegal as described in chapter 2.2. and if small changes in banner design result in noticeable differences in human behavior then more drastic changes are likely to produce those as well.

Once the preliminary banner designs were complete, a website for testing the banners was created and banner functionality was implemented, including a mechanism to save the answers to a database.

6.1. Determining the design goals

Based on the results of the cookie banner analysis in chapter 5.3, the banner mock-ups were designed to have the most important features of banners used in real life:

- The banner is placed in the middle of the website on top of a dark overlay. One of the options must be selected to continue browsing the website.
- Company logo on top of the banner.
- A headline with a neutral title.
- Two body text options, both stating how the data is used and with whom it is shared. Both texts have roughly the same length so that the length of the text does not make one of the texts more effortless to read. More of this in the next chapter.
- A link to a cookie settings.
- Filled buttons for accepting cookies. The “desired option” button was decided to be blue as it is commonly used in cookie banners and a fairly

neutral color compared the yellow, red and green. The exact shade of blue was decided to be #0069d9 as it is the shade of blue used for action buttons in the popular CSS framework Bootstrap. The “undesired option” button was decided to be white with a gray border and gray text inside it. The exact shade of gray was decided to be #767676 for both the text and the border of the button. This shade was chosen since it is the lightest shade of gray that is compliant with the WCAG accessibility guidelines for text (level AA).

- Font size was decided to be 1 rem (relative to default font size in browsers, usually defaults to 16px) for both body text and buttons since this is the default font size for web browsers. Headline text was decided to be bigger at 1.5 rem (by default 24px) and have bold font weight to signify its importance.
- The corners were slightly rounded, just as in many of the banners reviewed.

6.2. Banner text options

In order to test whether or not websites visitors actually read the banners, two versions of the banner texts were created. One was designed to closely resemble the tone and mention the same things as real-world banners. The other banner had the same first two sentences, but the tone changed after that. Instead of mentioning the benefits, it only spoke of the downsides: from the viewpoint of the protection motivation theory, we could speak of “heightened threat appraisal”. Care was taken to make this text threatening, but not so much that it would seem ridiculous. These texts will be referred to as the “encouraging text” and the “discouraging text”. The encouraging text is 576 characters in length whereas the discouraging text is 568 characters in length. This is slightly less than the 585 character average found in the banners tested in chapter 5. The English translations of both texts are found below. The original Finnish versions can be found in Appendix B.

Encouraging text: Cookies are small text files that are saved on your computer. If you wish, you can remove cookies from your browser’s settings.

We use cookies to collect anonymized statistical data about the visitor’s of the website. The data will only be used to improve the user experience of the website and to find and diagnose technical problems. By accepting cookies you help us to make our website more usable. The data will not be used for e.g. targeted advertising and we never share the data with third parties.

You can signal your consent by clicking “Accept all”.

Discouraging text: Cookies are small text files that are saved on your computer. If you wish, you can remove cookies from your browser's settings.

By accepting cookies you agree that we share your personal data with hundreds of other companies. We collect as much information about you as possible, including the social benefits you receive, your health information and your exact location. Our purpose is to sell the information and show you ads, including political ads, which are designed to be as effective as possible at altering your behavior.

You can signal your consent by clicking "Accept all".

6.3. Design process results

A total of eight permutations of the banner design were implemented. They are identical except for three factors: the content of the text, the colour of the reject button and whether the accept button was on the left or right. All these variations in individual elements are presented in figures 8 and 9. A settings page listing each cookie the website uses is also present.

Figure 8. *Cookie banner design with the encouraging text option and a nudging color scheme with a gray reject button on the right. There is a button for going to the settings as well, on the very bottom.*

Figure 9. *Cookie design with the discouraging text option and neutral button colors. Accept is on the right.*

6.4. Test website

To be able to test these cookie banners and to combine data a test was created. The test website belongs to an imaginary creative agency and was created using static site generator Hugo. Static site technology was chosen due to the availability of free hosting services and the generator due to the author's familiarity with the framework. To save time, a pre-built theme called Roxo (developed by StaticMania and licensed under the MIT license) was used on the website (https://github.com/StaticMania/roxo-hugo). Both the theme and the banner are fully responsive so test users would be able to complete the experiment both on desktop and mobile. Since the intention was to test the banners on a Finnish audience, the website was also translated to Finnish. The website was hosted on Netlify due to easy setup and the ability to use serverless lambda-functions in the backend. The support for lambdas was especially critical since they are a cheap (or in this case, free) alternative to more traditional hosting models and a backend of some kind was required to save the user's answers.

To make state management easier the banner was implemented using Preact instead of vanilla JavaScript. For every visit, the banner chooses a text, a button color and a button arrangement at random. Finally, the user's choice is saved in a Notion database for easy processing.

Figures 10, 11 and 12 represent how the website and the banner appear on desktop, tablet and mobile.

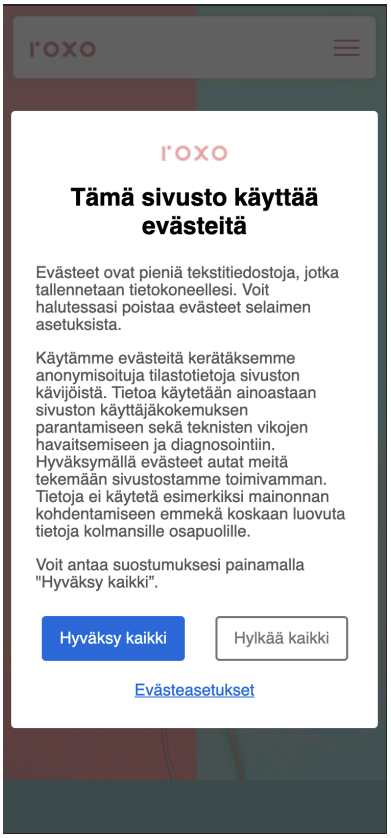


Figure 11. *This is how the banner appears on a mobile device.*

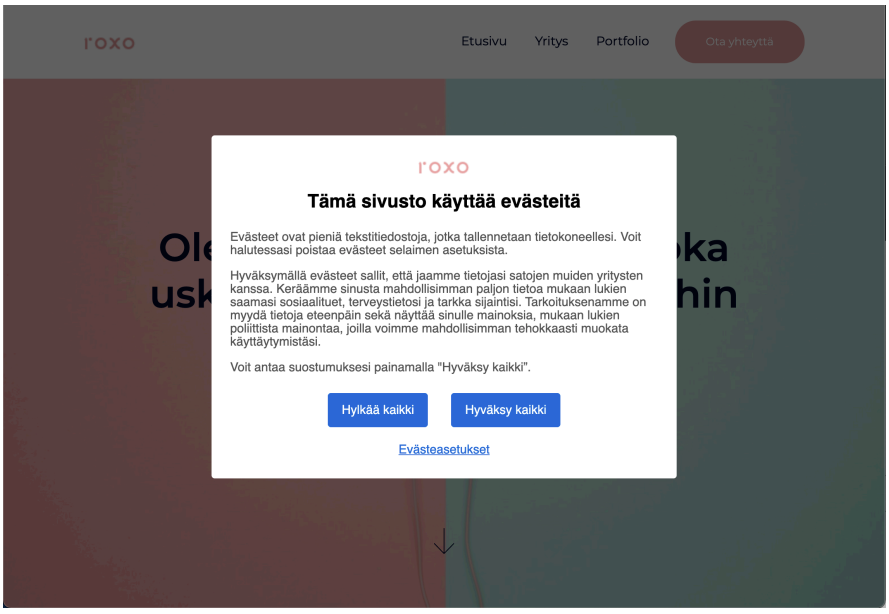


Figure 10. *This is how the banner appears on a computer.*

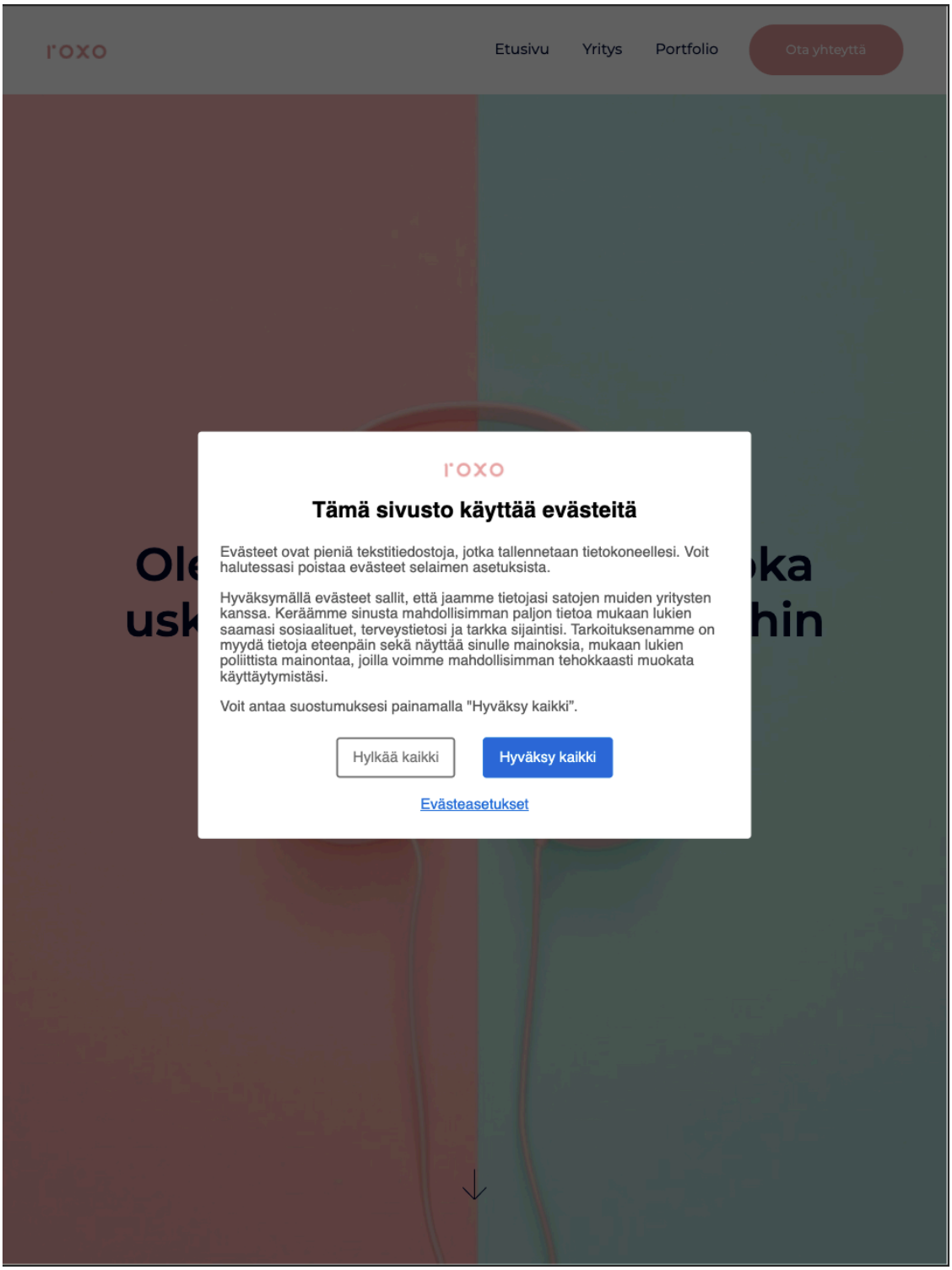


Figure 12. *This is how the banner appears on a tablet.*

7. STAGE 3: THE EXPERIMENT

This section covers the results of final experiment conducted for this thesis, the purpose of which was to answer research questions 2 and 3. Details on how the questionnaire was created and what questions were asked are covered in chapter 7.1. Chapter 7.2. covers the setup for the pilot study that was conducted before the actual survey. Chapter 7.3. gives a brief overview of the research participants. Chapter 7.4. describes the results and chapter 7.5. contains discussion of the findings. Chapter 7.6. covers the limitations of this research setup along with noteworthy information for anyone planning to undertake a similar research project in the future. Finally, chapter 7.7. covers the topic of research ethics.

7.1. Research method

In addition to the test website described in chapter 6 a second custom-built website was created for the experiment. The second website, from now on referred to as the questionnaire website, included six pages.

The first page provided information about the nature of the study, the author's name and asked for the user's consent to participate. The purpose of the study was told to be "researching how people interact on websites". This description was somewhat vague to avoid priming the users: any mention of cookies might have caused the participants to pay more attention to the cookie banner than they would normally do.

After the participant confirmed that he or she wishes to participate in the study and was over 15 years old at the time, a link to the second page became clickable. This page contained a questionnaire with basic demographic questions:

- Age in years
- Gender (male, female, other, unspecified)
- Education level according to the levels in the Finnish education system
- Employment status (student, employed, entrepreneur, unemployed, retired, other)
- The field the participant studied in, according to the National field of education classification by Statistics Finland (2016).

After the participant had submitted the answers, they were taken to the next page. On this page the participant was asked to take a computer self-efficacy measurement test. The questions in this test were the Finnish that were used by Howard (2014) with the exception that they were translated to Finnish. The purpose of this test was to help determine if experience with computers can help explain the other results.

After submitting the answers, the participant was shown a page with instructions and a link to the test website. The task given to all the participants was to find a contact form and then click the submit button without filling the form. Giving a task to the users was considered important as it added a layer of realism to the survey: it is unlikely that most people would browse the web specifically to click cookie banners.

On the test website the participant immediately faced a cookie banner with the option to either reject or accept cookies. The type of the banner along with the participant's choice was saved to a database.

After the participant had completed the task on the test website, they were automatically redirected back to the questionnaire page. On this page there were three questions: the first question was "Why did you choose to reject/ accept cookies" (reject or accept was displayed depending on which option the user had chosen). If the participant had chosen to accept cookies, the options were as follows:

- I want to see personalized ads or content
- Accepting cookies will help to improve the quality of the website
- I assumed that I would be blocked from the website if I had chosen to reject cookies
- I assumed that the website would not work as well if I had chosen to reject cookies
- I assumed that rejecting cookies would be more difficult than accepting them
- I assumed that the website would use cookies anyway
- I don't care if the website uses cookies or not
- I don't know
- Other

If the user chose to reject cookies, the following options were presented instead:

- I rejected cookies due to privacy reasons
- I assumed accepting cookies could make me more vulnerable to malware
- I feel that accepting would have offered me no benefits
- I don't care if the website uses cookies or not
- I don't know
- Other

The answer options were loosely based on the ones the ones used by Utz et al. (2019) and discussions with the pilot test participants (pilot tests are covered in chapter 7.2).

The second question on this page asked the participants to elaborate if they answered "Other" to the previous question or had something else to say concerning the matter. This was the only question to include a text field.

The last question on the page was "Let's assume that your browser had a setting that would let you either accept or reject all except necessary cookies on every website. After choosing either one of the options you will no longer see cookie banners on any website. All websites will also work in the same way regardless of which option you choose. If such a setting existed, which option would you choose?". Radio buttons with the following answer options were presented to the participants:

- Accept all
- Reject all (except necessary cookies)
- I don't know

This question basically describes one of the proposed solutions for the cookie fatigue problem. Using browser settings to signal consent has been proposed by several organizations (ICO, 2021; noyb, 2021). In practice the browser settings for declining or accepting cookies would most likely be more granular, with several cookie categories and the possibility to whitelist or blacklist certain domains. It is worth pointing out that as described in chapter 3.4. this question measures privacy intent or privacy attitude more than actual privacy behavior. Many people would probably leave this setting to whatever the default option is

(but as covered in chapter 2, due to GDPR it would have to be disabled by default).

Finally, after submitting these answers the participant was taken to a page that let them know that the survey was completed and thanked them for participating.

The original Finnish version of the questionnaire can be found in Appendix C.

7.2. Pilot studies

Five people were interviewed for the pilot study. The purpose of the pilot study was to look for technical problems in the questionnaire and on the test website and to verify that the questions were easy to understand. The interview consisted of five individual video conferences in which the participants filled the questionnaire while recording their screen. Afterwards, there was also a short unstructured interview with each participant. The participants were verbally informed that the purpose of the pilot study was to determine the viability of the study itself and their answers would not be recorded. The participants were also informed that they were free to not answer truthfully to any of the questions since anonymity could obviously not be guaranteed.

While there were no technical problems with the pilot study, an important observation was made. For some reason all participants except for one were observed to immediately click the accept button even though accepting offered them no benefit whatsoever and a button to decline was readily presented to them. Judging by how fast they accepted cookies it was obvious that they took no time in reading the text in the cookie notice. The small sample size did not enable further conclusions, but just in case a similar phenomenon would present itself in the actual test, a third questionnaire page was added to research website. The purpose of the third and final questionnaire page was to gather information to provide deeper understanding regarding the reasons behind the user's choices. We will call this page "motivation questionnaire".

A second pilot study was then conducted with three participants. In the second study the focus was to find technical problems with the third questionnaire page. None were discovered.

7.3. Participants and recruitment

The research participants were recruited by sharing the link to the survey on the social media website Linkedin and on subreddit r/Suomi along with the

Telegram channel of the university space technology club. Total number of participants was 318 out of which 189 people also answered the motivation questionnaire. It is worth pointing out that a significant number of participants exited the survey before answering the motivation questionnaire (figure 13). Of all the participants who clicked the cookie banner, 63% accepted cookies whereas that number was 55% for the participants who completed the survey in its entirety.

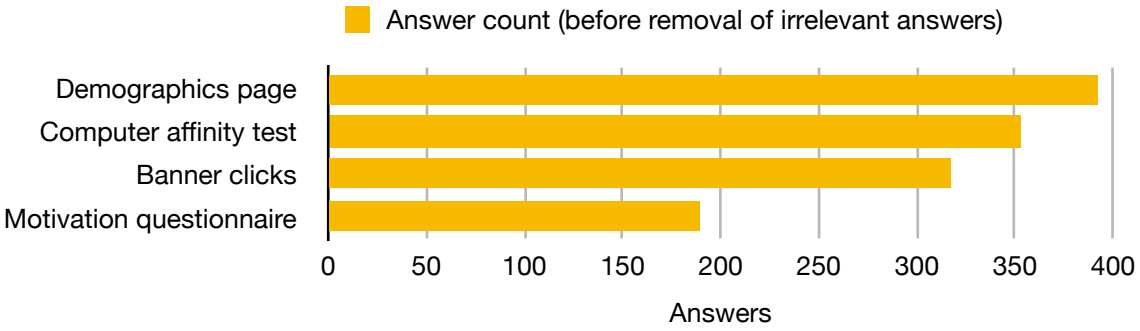


Figure 13. *Answers per page.*

Data collection took place during a two-week period between the 24th of September and the 8th of October of 2021. After the data collection period was over, all answers were reviewed to identify those that were potentially irrelevant. Two answers were clearly created by trolls (they were recognized through the use of excessive sexual references and insults towards the author's mother) and were removed. There were also ten answers in which the participant stated that they only accepted cookies because they assumed it would be necessary for research reasons. One answer was a test. One answer was a duplicate (both entries were removed as the participant made different consenting choices each time). One of the answers was malformed due to a technical error. All of these answers were removed as well. This brought the final answer counts to 302 and 173 respectively.

Demographic data was roughly the same in both datasets. The most common fields of education among the participants were ICT, engineering, manufacturing and construction. Around one half of the participants had studied in one of these fields. The average participant was also fairly young at 32 years, and around half of all participants were younger than 29 years of age. Roughly two thirds of the participants were male. See figure 14 for a more detailed breakdown.

The average score from the computer self-efficacy questionnaire for those who accepted cookies was 5,62 and for those that rejected cookies it was 5,76. The averages are fairly close to each other.

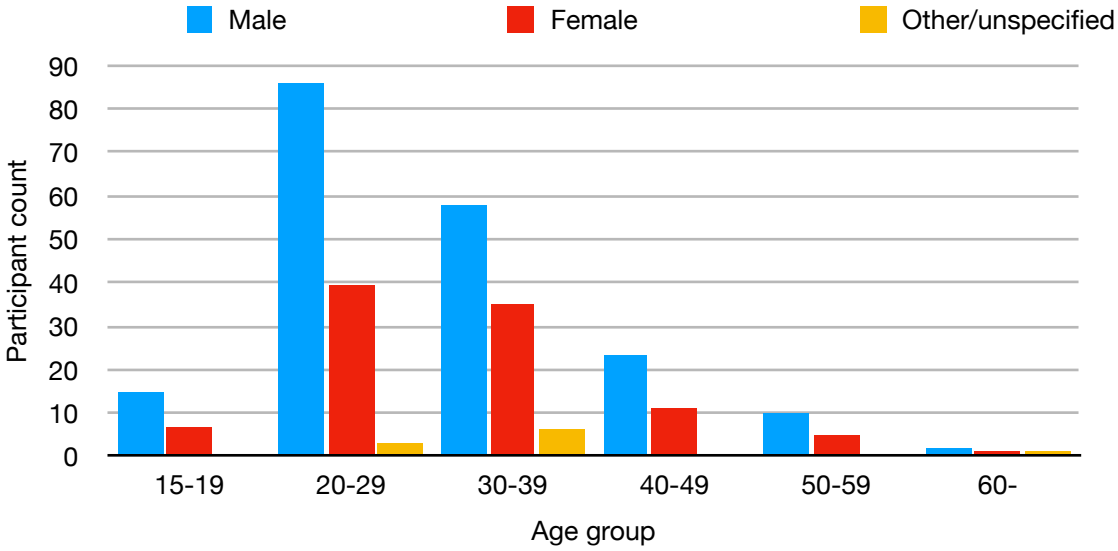


Figure 14. *Answers by age group. (All participants, after removal of irrelevant answers)*

Demographic data of the research participants is available in Appendix D.

7.4. Results

A one-tailed chi-squared test was used to determine if any of the tested properties had a meaningful effect on the consent rate. In every test the null hypothesis was that the variable being tested has no effect on the consent rate. To mitigate the multiple comparisons problem, the p-values obtained were then corrected using the Bonferroni correction method.

7.4.1. Answering research question 2

The results of the analysis can be seen in table 2. Most importantly we have to consider the p-value for the color of the buttons (highlighted in green) as it is the result that is most likely to be statistically significant with a corrected p-value of 0,089 which implicates a ~91% chance of the result not being random fluctuation. As no strict alpha level was chosen, multiple factors had to be taken into account when evaluating the significance of this result. First, the Bonferroni method is a rather harsh method for correcting the results in the sense that it has the tendency to cause type-II errors in which a false null hypothesis is mistakenly accepted. Second, the result obtained by Bauer et al. (2021) supports rejecting the null hypothesis. Third, the result that a blue button is more prominent next to a gray button than to another blue button makes logical sense. For these reasons the result was judged to significant enough to be used as a basis for conclusions.

Table 2: results of the statistical analysis (n = 302)

Factor to be tested	Odds ratio	p-value	Corrected p-value
Banner text		0,168516	0,505548
Color scheme	1,70	0,029831	0,089493
Button placement		0,572149	1

Based on the results, the test participants were 1,7 times more likely to accept cookies when the decline button was grey compared to both buttons being blue. This answers research question 2a. Text options or button placement had no statistically significant effect, which answers research question 2b. The data also suggests content of the text has no significant effect on decisions, which answers 2c.

7.4.2. Exploratory measurements for research question 3

After the research questions were answered, the data was further analyzed to discover any other correlations to explain the answers. The results of this analysis are seen in table 3 (FOE stands for field of education). All measured p-values are listed in table 3 with the clearly significant ones highlighted in green (those with a sample size of less than 20 were excluded). From these results we can see that that the only tested variable with an observed effect was education in business, administration and law. A person who has studied in one of these fields was nearly four times more likely than average to accept cookies.

Table 3: further results of the statistical analysis (n = 302)

Factor to be tested	Odds ratio	p-value	Corrected p-value
Gender: male		0,313760	1
Gender: female		0,173875	1
Education: high school / vocational school		0,197462	1
Education: bachelor's degree		0,370827	1
Education: master's degree		0,444910	1
FOE: Generic programmes		0,780103	1
FOE: Arts and humanities		0,112900	1
FOE: Business, administration, law	3,99	0,001367	0,01367

Factor to be tested	Odds ratio	p-value	Corrected p-value
FOE: ICT		0,770282	1
FOE: Engineering, manufacturing and construction		0,197462	1

The questionnaire which asked for reasons behind accepting cookies gives some answers but also raises more questions. Reasons for declining cookies are fairly straightforward: Out of 78 participants 68 stated that they declined due to privacy reasons, and 59 also stated that there was no conceivable benefit from accepting cookies. The other options were chosen by fewer than 7 participants each (figure 15). The same themes were repeated in the 11 open-ended answers: *In most cases, I only accept necessary cookies on sites I visit because I don't want my information to be used e.g. for targeting ads or similar purposes.* Some people also seemed to feel like they were fighting someone who was irritating them: *I'm annoyed by the cookie acceptance requests, so I feel like I'm getting back at them when I don't accept.*

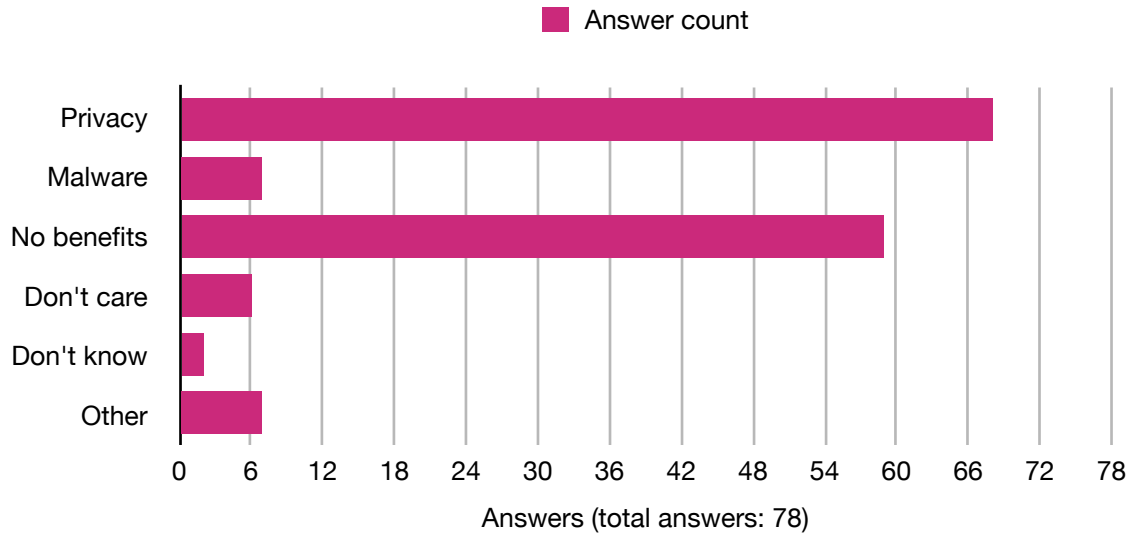


Figure 15. *Reasons given for declining cookies.*

Reasons for accepting cookies were more diverse (figure 16). It is clear that most participants did not accept cookies because they excepted to receive some kind of a benefit from them. Eight out of 95 participants stated that they accepted because they want to see relevant ads. This is peculiar, as half of the eight were shown a cookie banner that specifically stated that the information collected would *not* be used for targeted advertising. Only eleven participants wanted to help in improving the quality of the test website. These reasons did not seem to be very important even among the participants who chose these

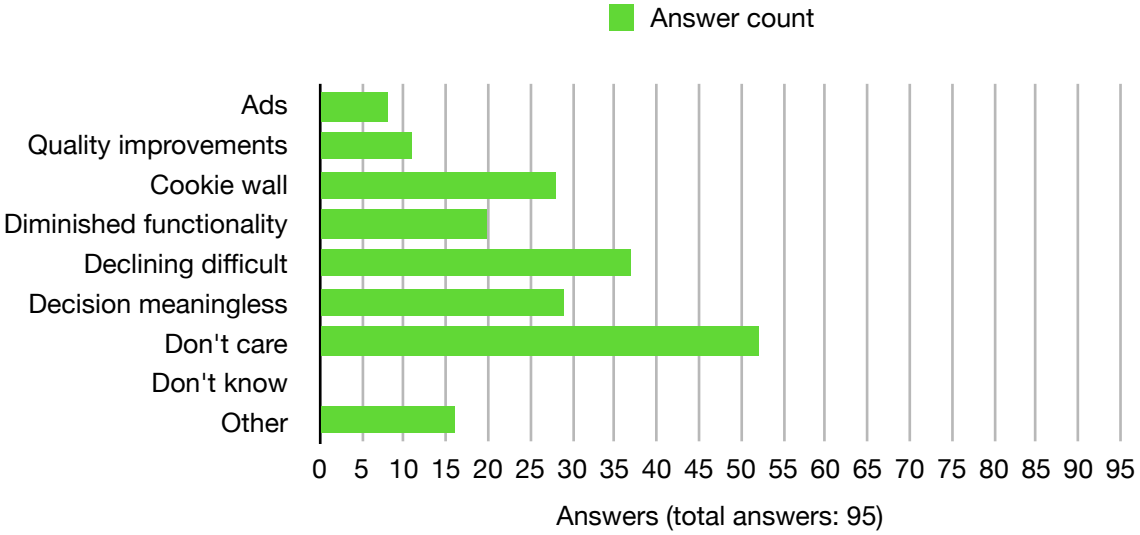


Figure 16. *Reasons given for accepting cookies.*

options: only two out of the eight and five out of the eleven would have accepted non-essential cookies through browser settings.

Many participants believed that there would be some kind of harm in not accepting cookies. A total of 28 people stated that they expected to be blocked from the website and 20 participants believed that the website would not work as well had they chosen to reject cookies.

A total of 37 people stated that they believed declining cookies to be more difficult than accepting cookies. From this we can deduct that at least these 37 people did not even read the button labels or for some reason assumed that “Reject all” would mean something other than rejecting all.

There were also clear signs of indifference towards the use of cookies. 29 participants considered their decision to be meaningless in the sense that the page would use cookies anyway and might not respect their choice. This indicates a general distrust towards data collection practices. 52 participants stated that they simply don’t care about if the website uses cookies or not. Despite this, 38 out of the 52 stated that they would have chosen to refuse cookies in browser settings.

The final question about whether or not the participant would accept or decline cookies using dedicated browser settings yielded an interesting result. While it would be logical to assume that people would make the same choices in the settings and on the website, this was not the case among those who accepted cookies. This is demonstrated in figure 17. 80% of the participants who accepted cookies answered they would choose differently in settings.

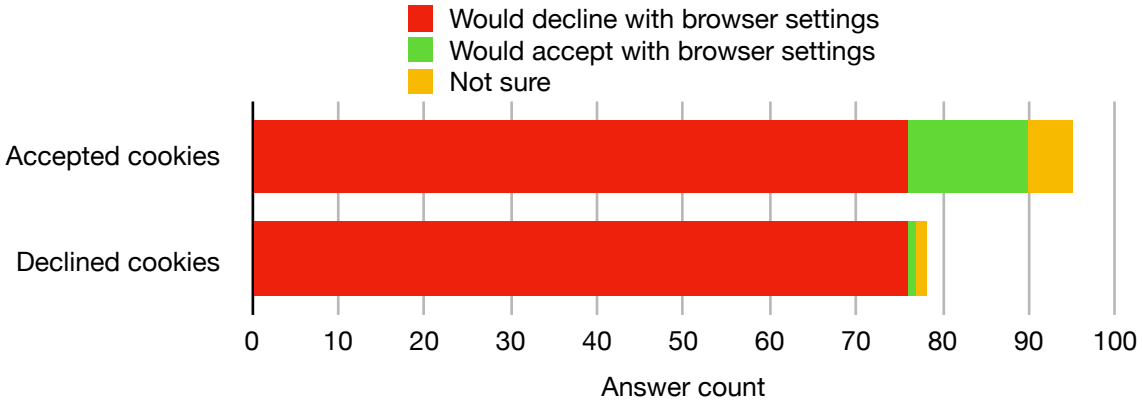


Figure 17. *Choice on website vs. choice in settings.*

The open-ended questions did not offer conclusive answers to understanding the results. Of the 21 who gave an open-ended answer five participants made references to "automatic" decision making: *I took action completely automatically and didn't even realize there was a cookie banner on the site.* Some also expressed frustration with the banners: *I just click on the option that makes the distracting window go away. / I just wanted to get the annoying window out of sight.* Some also repeated their observation that many websites do not work or allow them to enter without accepting cookies.

There was also an answer that helps to explain the high cookie acceptance rate among those whose field of education is business, administration or law: one research participant stated that she works in marketing and always accepts cookies out of solidarity towards her colleagues since *"things get complicated if advertising and content cannot be targeted to a specific audience".*

7.5. Discussion

With the results obtained from the experiment it is possible to answer the remaining two research questions. First, the answer to RQ2a is that the color of the accept/decline buttons can indeed have an effect on if a website visitor accepts cookies or not. The location of the buttons did not have a statistically significant effect, answering RQ2b. As the amount and the purpose of information collected by the website did not have a statistically significant effect on user choice either, the answer to RQ2c is that text changes do not significantly change user behavior. The results are in line with the results obtained by Bauer et al. (2021) who confirmed that a highlighted accept-button increased consent amounts and Van Bavel and Rodríguez-Priego (2016) who discovered that banner text had virtually no effect on user decisions. This leads

to the conclusion that color of the buttons has more effect on consent rates than what people are consenting to.

7.5.1. Reasons for accepting cookies

While it was quite clear that people reject cookies for privacy reasons and because there was no perceived benefit from accepting them, the reasons behind accepting cookies are highly contradictory.

First of all, why did so many people believe there would be a cookie wall on the website? This is more or less inexplicable as cookie walls are illegal, none of the Finnish websites reviewed for this thesis had one and it was not stated anywhere in the survey that using the test website would require accepting cookies. Possible explanations include that 1) there is a significant number of Finnish websites that have illegal cookie walls, 2) there is a significant number of foreign websites that are popular among Finnish users that have cookie walls, or 3) participants assumed that accepting cookies would be required for research reasons. Some people did state that they only accepted cookies because they assumed it was necessary for the alleged research software on the website to work correctly. While these answers were removed from the source data before this analysis was conducted, perhaps there were more people under the same assumption who just didn't bother writing an open-ended response confirming it. Explaining why a significant number people are under the impression that any cookie notice serves as a cookie wall will be an interesting topic for future research. Same goes for explaining why people are under the assumption that declining cookies would somehow cripple the website; as essential cookies are exempt from the regulation, there is no reason (except for ignorance) for anyone to make a website that blocks essential cookies based on user choice.

The most common "reason" for accepting cookies was that the participant does not care. This is inexplicable, as 38 out of the 52 would have refused cookies using browser settings even though the option "I don't know" was also available for them to select. So, in the browser setting scenario they apparently would care, at least a little. Could there be something in the cookie banner itself that causes them to be indifferent about the use of cookies? Is it that rejecting cookies is generally more difficult than accepting them? If so, why didn't most of them either reject cookies outright or choose the answer option "I thought declining would be more difficult than accepting cookies"?

Around a third of the participants stated that they believed refusing cookies would be more difficult than accepting them. This is a logical assumption, as on most websites refusing cookies is indeed more difficult than accepting

them. Only 6 of the 50 websites reviewed for this thesis offered an easy option to reject cookies. We can, however, also draw the conclusion that these people did not read the cookie banner as the option to reject all cookies was clearly visible.

Overall, there are two possible ways we can choose to interpret these contradictory results: 1) there is an undiscovered pattern to explain the results that was simply not found by the author or 2) the data is just what it appears to be: contradictory. Since we have already explored the possibility of there being a pattern, let's entertain the thought of the data being contradictory and irregular and explaining why that could be. As stated in chapter 3.4, if a person takes an action that is not in line with their beliefs or the action is taken for no reason at all, they tend to come up with some kind of explanation or justification for it. This questionnaire conveniently provided multiple such justifications to the participants in the form of the checkbox answers to the questionnaires. It is possible the participants resolved their cognitive dissonance by choosing any answer that rationalized their actions, resulting in the inconsistent and contradictory answers we are seeing.

To summarize, the answers from cookie-accepting participants in the motivation questionnaire are highly contradictory. Many of the participants gave valid reasons for accepting cookies, yet stated they would decline cookies in browser settings if a suitable setting was available. Many also seemed to completely ignore the choices that were available on the banner and made their choice based on what choices they assumed to be available.

7.5.2. Explaining high consent rates among people educated in business, administration or law

While this sample size is too small for any conclusive results, we can speculate on why people with education in business, administration or law are significantly more likely than average to accept cookies. This might be because people who work in marketing are likely to fall to this category. According to the open-ended answers, marketers might feel that they would achieve less satisfactory return-on-investment without cookie-related tracking technologies. Marketing personnel also rely on cookie-based web analytics to measure how effective their campaigns are and perhaps to prove to the management that marketing is indeed something that is worth investing in. Due to these reasons a digital marketer might think he or she is helping colleagues by accepting cookies. It would also most likely be difficult to work on this field if one considers cookies or data collection to be something that is harmful.

7.5.3. Evidence of conditioning

This research project has yielded an unexpected result that is so significant that it renders the answers to the second research question almost irrelevant. When the research questions were chosen, an assumption was made that cookie banners can have two significant properties that can influence the decision made by a website visitor: its information content and its visual elements and design (see chapter 4.1. for a more detailed explanation about the research questions). However, the strangest pattern appears in the results that suggests that there is a third property. The overwhelming majority, that is, 80% of the research participants who accepted cookies stated that they would have rejected cookies if they could have made what is essentially the same choice in browser settings. Why would so many people make a different decision on a website and in browser settings? It makes no sense whatsoever.

Unless there is no decision. Through the writing of this thesis, it has been assumed that users would make a decision of some kind when facing a cookie banner. Perhaps not a very informed or reflective decision, but at least some kind of assessment between the options would occur. The possibility of there being, in fact, no decision at all has been almost completely ignored. It seems that when facing the banner roughly 50% of all research participants rushed to find the Accept-button despite their apparent aversion towards accepting cookies. If they had been making what we would call a decision, they would surely have read at least the labels of the two big buttons, one of which contains the very choice they would have made in browser settings if given the opportunity. But no, they went for the Accept-button guided by their Automatic/System 1 process.

Why the Accept-button then? All available research suggests that on every website that has a cookie banner there is also a button for accepting cookies with one click. To cite the one with the largest sample size that was found in the literature review, Nouwens et al. (2020) scraped ten thousand websites in the UK and every single one of them had an accept button on the first layer. On every website tested in chapter 5 the results were no different. Options to decline cookies are often hidden or non-existent. Therefore if one wishes to view the contents of an arbitrary website with a cookie banner, the most efficient way of doing so is to assume there is an an accept button, find it as fast as possible and click it. It will work regardless of how the banner is designed and as it is simple task, in time it will most likely be delegated to the automatic decision-making system. It seems to be that the large number of websites that make refusing cookies difficult has effectively conditioned people into accepting cookies even on websites where the nudges are not present.

This effect also appears to be far stronger than the nudging effects of banner design or content. The survey results in which some people report making the decision “automatically” also support this conclusion.

This is not the first time that this idea has been brought up in related works, either. Graßl et al. (2021) also speculated with the idea, stating that while nudges are thought to be functional only when the nudge is in place it might not always be so. According to Hertwig & Grüne-Yanoff (2017) if a nudge is encountered repeatedly, or lasts for a long time, possibly years (in this case both conditions might well be true) a nudge may turn into a behavioral routine that can persist even if the choice architecture is removed.

Due to to sheer magnitude of this effect it is difficult to find any possible alternative explanations for it. The only conceivable one is that the vast majority of the research participants accepting cookies do not do so on other websites, but made an exception for this website. There is little evidence to support this, except for the fact that some might have been worried that declining cookies would result in the research software not being able to record their answers. However, let us assume for a second that everyone who accepted cookies due to the fear of a cookie wall or diminished website functionality made their decision based on that belief. That would still only explain the behavior of 30 people out of 76. No alternative reason that would explain the participants behavior in full was observed. Therefore the answer to RQ3 is that there is evidence suggesting conditioning may have an effect on behavior.

7.6. Limitations

First of all, the survey was conducted in the Finnish language, which means it is logical to assume that most people answering the survey were Finnish. Results might be different if the survey had been conducted in another language and/or in another area. The effects observed might be weaker, stronger or nonexistent depending on what kind of cookie banners the participants are used to seeing.

For some reason, more than half of the participants reported that their field of education was either ICT or technology. This number is disproportionately high when compared with the entire population of Finland. This might be caused by the fact that many of the author’s LinkedIn connections IT professionals. Also, around two thirds of the respondents were male. The demographic factors that were analyzed in this experiment did not seem to correlate with the likelihood to accept cookies, however.

Asking people why they accepted cookies does not seem to yield very useful results when the answer options are binary (yes/no). The results of this survey indicate that while people might give many reasons for accepting cookies, some reasons can be significantly more important than others. On retrospect this is rather obvious but nevertheless it is something to keep in mind in future experiments. For example, a Likert scale or interviews might result in more detailed and useful answers.

Also, significantly more people clicked the cookie banner than answered the motivation questionnaire, there was a ~40% drop in the number of answers. It is not unexpected that some research participants drop out in the middle of the survey, but 40% is still a rather large number: the other pages did not see such a large number of people leaving the questionnaire. This was previously demonstrated in figure 13. One participant pointed out to the author that reading the instructions about the task to do on the test website was necessary for the websites to work as intended: after proceeding to the test website there was no option to go back and read the instructions again. While the task was fairly simple, it is possible that some people ignored or forgot the instructions and consequently were unable to answer the motivation questionnaire. Data from Hotjar supports this, as some people seemed to browse the website in a random manner. With this research setup the reasons behind cookie choices of people who do not read instructions were not recorded, causing a selection effect of unknown strength. During the data collection period there was an opportunity to change the instructions and perhaps add a confirmation checkbox to help ensure more people would read the instructions. The author ultimately decided against it, reasoning that in the end a predictable bias would be preferable to an unpredictable one. For better or worse, the instructions remained the same during the entire data collection period. The drop could also be caused due to a technical error that prevented the banner from working properly. Such errors could possibly be caused by an adblocker or an adblocker extension script that is designed to automatically accept all cookies. The banner was originally tested to work even with an adblocker (uBlock Origin) enabled, but not with custom scripts or extensions specifically designed to block cookies such as *I don't care about cookies* (Kladnik, 2021).

It is known (see chapter 3.4.) that the perceived trustworthiness of a website might have an effect on the choice people make when facing a cookie banner. In this case the test website was "endorsed" by a known university. Moreover, when reaching the test website the participants had already decided to trust this university by completing two questionnaire pages. Ten people directly stated that they only accepted cookies because they knew they were

participating in a research project and assumed that accepting cookies was necessary for the test page to work correctly. For this reason it can be hypothesized that in general people are more likely to accept cookies on the test website than, for example, on an eCommerce website they are visiting for the first time. Testing a cookie banner on real website might therefore result in somewhat different answers. This approach was considered for this project as well, but conducting research on participants that are oblivious to the fact that they are being observed is ethically problematic. It would have needed approval from Tampere University Ethics Committee which does not process requests related to master's theses making this approach impossible. Also, the approach taken here made it possible to attach a questionnaire to the project. This resulted in data that would have been difficult to obtain from users that are unaware of the experiment.

7.7. Research ethics

All of the research participants were made aware of the fact that they were research participants by first directing them to a web page with information about the study. The participants were told that participating is anonymous and no personal data would be collected. The diagnostic tool Hotjar was installed on the test website, and the participants were informed of this beforehand with a link to Hotjar's privacy policy. The participants were also informed that participation is entirely voluntary and they were free to quit at any point without negative consequences. It was not possible for a participant to proceed to the study without first checking a box confirming that the instructions had been read. Due to the nature of the study it was not possible to tell the participants exactly what was being tested: they were told that the study will analyze their behavior on a website and all necessary information would be collected automatically. This is ethically somewhat problematic, but also necessary to avoid the priming effect and to obtain any meaningful results. The minimum age for participants was 15 years.

The answers were saved in a password-protected database to which only the author had access to. When analyzing the results the problem of multiple comparisons was counteracted using the Bonferroni method. The author did not receive funding from any source to write this thesis.

8. CONCLUSIONS

The research in this thesis was based on three research questions. The first research question focused on gathering data from real-world cookie banners to produce an archetype that could be tested for the remaining two research questions. The second question was how the purpose and amount of information collected with cookies affects consent rates compared to changes in button color and placement. The final research question was focused on discovering any possible factors other than banner design or banner text that might influence user behavior.

8.1. Key findings and contributions

The results of this thesis present several problems with both cookie banners in general and the validity of consents obtained using cookie banners. Even when a cookie banner is perfectly compliant with all regulations, the validity of the consent can be questioned.

The results of the website review suggest that only few websites comply with the law. All of them also used dark patterns of some kind to guide the user towards selecting privacy-unfriendly options. This is no doubt in part due to Traficom's long-lasting non-existent enforcement of the said law.

Subsequent experimentation revealed that users were somewhat more likely to accept cookies if the decline button was grey and the accept button blue, as opposed to both buttons being blue. Placing the accept button on the left side of the decline button had no statistically significant effect on consent rates compared to having the accept button on the right.

Of the two banner texts one stated that only the bare minimum of information is collected to improve the service, it would not be used for advertising purposes and the data would not be shared with third parties. The other stated that even most sensitive information such the users health information, exact location and information of social benefits would be collected, sold to third parties and used for all kinds of advertising, including political advertising. No mention of any benefits to the user was included (unless said advertising is considered a benefit). The content of the text had no statistically significant effect on consent rates. This leads to the conclusion that the color of the buttons has more effect on consent rates than what the user is asked to consent to.

Demographic factors were determined to have no statistical effect on the results, with the exception of one. If a person's field of education was business, administration, or law the person was significantly more likely to accept cookies. This is possibly due to the fact that people who work in marketing (or more specifically, digital marketing) might have received education in the field of business or administration. It would make sense that in general marketers are more likely to accept cookies since they are well familiar with the benefits cookies offer for website operators. On the other hand, if a person believes cookies are harmful it is unlikely that he or she would be very willing to work in digital marketing.

An unexpected yet very strong effect influencing the behavior of the test users was also discovered. 80% of the users who accepted cookies stated that if they would be presented with a possibility to make the same choice in browser settings they would have declined cookies. It seems that the banner itself is something that influences the user's decisions instead of any specific detail in the banner. According to Hertwig & Grüne-Yanoff (2017) repeated nudges (such as the ones seen in cookie banners) can become a behavioral routine which can remain even if the nudging choice architecture is removed. In this case the nudging choice architecture refers to the widely-used cookie banners that make declining cookies more difficult than accepting them. This theory of behavioral conditioning is further supported by test subjects' behavior in the pilot test, apparent indifference towards the text changes and the contradictory answers to the questionnaire asking users to specify why they accepted cookies.

8.2. Legal implications and recommendations to policy makers

The results of this work suggest that a consent to the use of cookies obtained by the use of a cookie banner is invalid. Based on the results the vast majority of people makes their cookie decisions based on anything but what their personal data is used for. Based on the results it also seems that a significant number of people would accept nearly any statement as long as it is provided in the form of a cookie banner. This clearly indicates that the consent is not "informed" as demanded by GDPR. Due to the fact that most participants stated that they did not actually wish to accept cookies even after clicking the button to accept, we have to conclude that clicking the button to accept is, in fact, not even an "indication of wishes". For these reasons, the following measures are recommended by the author:

1. Ban cookie banners. Since the results suggest that even a banner that complies with regulations perfectly cannot be used to obtain informed consent, this is the only option remaining if consumer privacy is considered to be worth protecting. Laws requiring consenting to cookies might even have done more harm than good in the sense that a banner can now be used to get users to “consent” to anything as demonstrated before.

2. Implement legislation for browser-based cookie controls that allow users to choose what type of cookies they wish to accept. This would likely solve the issue of consent fatigue.

3. Enforce the regulations. Any form of privacy legislation that is not enforced is useless and possibly counterproductive. The observed conditioning effect might even be a direct consequence of lax enforcement of the laws: since banners in which declining cookies is illegally difficult have been allowed to exist for years, a significant number of people now seem to act as all banners were of illegal design.

4. Ban user interfaces that ask the user to change their browser settings concerning cookies or whitelist websites. Otherwise it is quite possible that the legislation will simply end up creating a new banner problem to replace the old one, for an example see figure 18. Website operators have strong incentives to collect data and some will undoubtedly try to find new ways to obtain “consent” for data processing and the use of cookies. Other possible loopholes should be addressed as well.

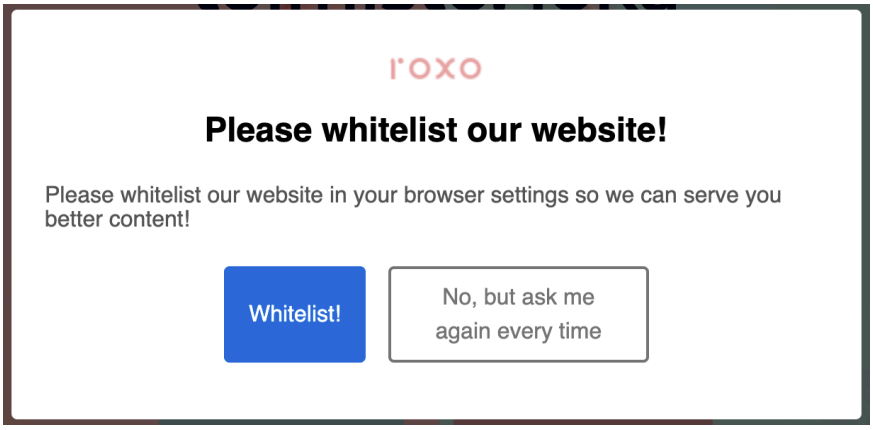


Figure 18. *A whitelist banner might replace cookie banners unless explicitly banned.*

8.3. Future work

Since it would appear that the conditioning effect is the most important driver behind user's behavior, it is among the most important topics for future work. More research is needed to confirm both its existence and to determine how strong the effect is. It might also be worthwhile to explore how long this effect will last and if there is a user interface design that could undo the conditioning. This thesis also focuses more on determining why people accept cookies than why people decline cookies: it is possible that some people that decline cookies are similarly conditioned and will try to do everything in their power to find a decline button when presented with a banner regardless of the banner's content. This is also an interesting focus area for future research.

The results of the questionnaire where people were asked why they accepted cookies was also highly contradictory. A more detailed study on consisting of follow-up interviews should be conducted. Such a study would be helpful in determining if test participants just come up with a way to rationalize accepting cookies after being conditioned to do so for years or if there is some other reason for the observed inconsistencies.

A statistical test should also be performed on data from the computer self-efficacy test. The differences in averages for people who accepted cookies and people who declined cookies is slight, but the possibility of correlation cannot be excluded without further testing. Cookie acceptance rates among marketers compared to the rest of the population are also something to test. In this thesis it is speculated that marketers are more likely than average to accept cookies, but there is not enough material to be certain.

Finally, similar research should be conducted across Europe since the legislation is pan-European and there may be differences on how people from different countries react to cookie banners. The results also depend on what kind of cookie banners are in use in different areas.

REFERENCES

Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C., Preneel, B. (2015). *Facebook Tracking Through Social Plug-ins. Technical report prepared for the Belgian Privacy Commission.* KU Leuven. Available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf. Link retrieved October 3, 2021.

APA Dictionary of Psychology (2021). *Rationalization.* American Psychological Association. Available at https://dictionary.apa.org/rationalization. Link retrieved October 21, 2021.

Adobe Analytics (2021). *Adobe Analytics.* Adobe. Available at https://business.adobe.com/products/analytics/adobe-analytics.html. Link retrieved October 3, 2021.

Amendment of Privacy and Electronic Communications Directive. Directive 2009/136/EC. European Parliament and Council. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=en. Link retrieved October 3, 2021.

Aunola, V. (2020). *Maailman arvokkain yhtiö on Aramco – Kone jatkaa Suomen ykkösenä.* Viisas Raha. Available at https://viisasraha.fi/Markkinat/Maailman-arvokkain-yhtiö-on-Aramco-–%C2%A0Kone-jatkaa-Suomen-ykkösenä. Link retrieved October 14, 2021.

Avast (2021). *Data Brokers: Everything You Need to Know.* Avast. Available at https://www.avast.com/c-data-brokers. Link retrieved October 4, 2021.

Barth, A. (2021). *HTTP State Management Mechanism.* Internet Engineering Task Force. Available at https://datatracker.ietf.org/doc/html/rfc6265. Link retrieved October 3, 2021.

Bauer, JM., Bergstrøm, R., Foss-Madsen., R. (2021). *Are You Sure, You Want a Cookie? The Effects of Choice Architecture on Users' Decisions about Sharing Private Online Data.* Computers in Human Behavior, Volume 120, Article 106729. https://doi.org/10.1016/j.chb.2021.106729

Bornschein, R., Schmidt, L., Maier, E. (2020). *The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie*

Notices. Journal of Public Policy & Marketing, Volume 39, Issue 2, Pages 135-154. https://doi.org/10.1177/0743915620902143.

Brandom, R. (2021). *Facebook shut down German research on Instagram algorithm, researchers say.* The Verge. Available at https://www.theverge.com/2021/8/13/22623354/facebook-instagram-algorithm-watch-research-legal-threat. Link retrieved October 13, 2021.

Brave Ads (2021). *Expand your business with Brave Ads.* Brave. Available at https://brave.com/brave-ads/. Link retrieved October 4, 2021.

Brignull, H. (2011). *Dark Patterns: Deception vs. Honesty in UI Design.* A List Apart. Available at https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/. Link retrieved October 11, 2021.

Brignull, H. (2021). *What Are Dark Patterns?* Dark Patterns. Available at https://www.darkpatterns.org. Link retrieved October 10, 2021.

Built With (2021a). *Websites using Google Font API.* Built With. Available at https://trends.builtwith.com/websitelist/Google-Font-API. Link retrieved October 3, 2021.

Built With (2021b). *Google Analytics Usage Statistics.* Built With. Available at https://trends.builtwith.com/analytics/Google-Analytics. Link retrieved October 3, 2021.

Burgess, M. (2020). *What is GDPR? The summary guide to GDPR compliance in the UK.* Wired. Available at https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018. Link retrieved October 3, 2021.

Cambridge Dictionary (2021). *Rationalization.* Available at https://dictionary.cambridge.org/dictionary/english/rationalization. Link retrieved October 21, 2021.

Case C-673/17 (2019). *Judgement of the Court.* The Court of Justice of the European Union. Available at https://curia.europa.eu/juris/document/document.jsf;jsessionid=46B7E8464BEE3EDA25DFBD221C4F9986?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2911961. Link retrieved October 3, 2021.

Chabris, C., Simons, D. (2010). *The invisible gorilla: And other ways our intuitions deceive us.* Crown Publishers/Random House.

Chaiken, S., Trope, Y. (Eds.). (1999). *Dual-process theories in social psychology.* The Guilford Press.

CNIL (2020a). *Cookies: financial penalties of 60 million euros against the company GOOGLE LLC and of 40 million euros against the company GOOGLE IRELAND LIMITED.* Commission Nationale de l'Informatique et des Libertés. Available at https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland. Link retrieved October 3, 2021.

CNIL (2020b). *Cookies: financial penalty of 35 million euros imposed on the company AMAZON EUROPE CORE.* Commission Nationale de l'Informatique et des Libertés. Available at https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core. Link retrieved October 3, 2021.

Davies, J. (2019). *After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue.* Digiday. Available at https://digiday.com/?p=317843. Link retrieved October 4, 2021.

Decision H1515/2021. Administrative court of Helsinki.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). European Parliament and Council. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN. Link retrieved October 3, 2021.

Downs, A. (1957). *An economic theory of democracy.* New York: Harper & Brothers.

ecommerceDB (2021). *Store Ranking & Overview.* Statista. Available at https://ecommercedb.com/en/ranking/fi/all. Link retrieved October 14, 2021.

EFF (2021). *Cover your Tracks.* Electronic Frontier Foundation. Available at https://coveryourtracks.eff.org/learn. Link retrieved October 26, 2021.

European Data Protection Board (2020). *Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1.* European Union. Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Link retrieved October 3, 2021.

Eurostat (2020). *Data Browser.* European Union. Available at https://ec.europa.eu/eurostat/databrowser/view/TPS00001/bookmark/table?lang=en&bookmarkId=c0aa2b16-607c-4429-abb3-a4c8d74f7d1e. Link retrieved October 3, 2021.

Facebook for Developers (2021). *Facebook Pixel. Implementation.* Facebook. Available at https://developers.facebook.com/docs/facebook-pixel/implementation/. Link retrieved October 10, 2021.

Facebook Investor Relations (2021). Facebook Reports Fourth Quarter and Full Year 2020 Results. Facebook. Available at https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx. Link retrieved October 4, 2021.

Fiebrandt, S. (2018). *What are cookies? What are the differences between them (session vs. persistent)?* Cisco. Available at https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.html. Link retrieved October 3, 2021.

Forbrukerrådet (2018a). *Filing complaint against Grindr's sharing users' HIV-status and sexual preferences.* Norwegian Consumer Council. Available at https://www.forbrukerradet.no/side/filing-complaint-against-grindrs-sharing-users-hiv-status-and-sexual-preferences/. Link retrieved October 4, 2021.

Forbrukerrådet (2018b). *Report: Deceived by design.* Norwegian Consumer Council. Available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf Link retrieved October 10, 2021.

Gartner (2021). *Data Broker.* Gartner. Available at https://www.gartner.com/en/information-technology/glossary/data-broker. Link retrieved October 4, 2021.

Gerber, N., Gerber, P., Volkamer, M. (2018). E*xplaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior.* Computers & Security, Volume 77, Pages 226-261. https://doi.org/10.1016/j.cose.2018.04.002.

Google Ads Help (2021a). *About your data segments.* Google. Available at https://support.google.com/google-ads/answer/2453998?hl=en. Link retrieved October 3, 2021.

Google Ads Help (2021b). *Tag your website using Google Ads.* Google. Available at https://support.google.com/google-ads/answer/2476688?hl=en. Link retrieved October 3, 2021.

Google AdSense (2021). *We value your content.* Google. Available at https://www.google.com/intl/en_uk/adsense/start/. Link retrieved October 3, 2021.

Google Analytics (2021). *Get to know your customers.* Google. Available at https://marketingplatform.google.com/about/analytics/. Link retrieved October 3, 2021.

Google Analytics Help. (2021). *[GA4] Set up Analytics for a website and/or app.* Google. Available at https://support.google.com/analytics/answer/9304153?hl=en&ref_topic=9303319#zippy=%2Cadd-the-global-site-tag-directly-to-your-web-pages. Link retrieved October 10, 2021.

Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., Buijzen, M. (2021). *Dark and Bright Patterns in Cookie Consent Requests.* Journal of Digital Social Research, Volume 3, Number 1, Pages 1-38. https://doi.org/10.33621/jdsr.v3i1.54

Hern, A. (2014). *Why Google has 200m reasons to put engineers over designers.* The Guardian. Available at https://www.theguardian.com/technology/2014/feb/05/why-google-engineers-designers. Link retrieved October 5, 2021.

Hern, A. (2018). *Cambridge Analytica: how did it turn clicks into votes?* The Guardian. Available at https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie. Link retrieved October 4, 2021.

Hertwig, R., Grüne-Yanoff, T. (2017). *Nudging and Boosting: Steering or Empowering Good Decisions.* Perspectives on Psychological Science. Volume 12, Issue 6, Pages 973–986. https://doi.org/10.1177/1745691617702496

Hindermann, C. M. (2018). *Price Discrimination in Online Retail.* ZBW – Leibniz Information Centre for Economics, Kiel, Hamburg. http://hdl.handle.net/10419/181294

Holson, L. M. (2009). *Putting a Bolder Face on Google.* The New York Times. Available at https://www.nytimes.com/2009/03/01/business/01marissa.html. Link retrieved October 5, 2021.

Hotjar (2021). *Understand how users behave on your site, what they need, and how they feel, fast*. Hotjar. Available at https://www.hotjar.com. Link retrieved October 3, 2021.

Howard, M. (2014). *Creation of a Computer Self-Efficacy Measure: Analysis of Internal Consistency, Psychometric Properties, and Validity.* Cyberpsychology, behavior and social networking, Volume 17, Issue 10, Pages 677-681. https://doi.org/10.1089/cyber.2014.0255.

ICO (2021). *ICO to call on G7 countries to tackle cookie pop-ups challenge.* UK Information Commissioner's Office. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/09/ico-to-call-on-g7-countries-to-tackle-cookie-pop-ups-challenge/. Link retrieved October 14, 2021.

Jeong, S. (2020). *Tinder charges older people more.* CHOICE. Available at https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/tinder-plus-costs-more-if-youre-older. Link retrieved October 4, 2021.

Kahneman, D. (2011). *Thinking, fast and slow.* Farrar, Straus and Giroux.

Kaspersky (2021). *What is an IP Address – Definition and Explanation.* Kaspersky. Available at https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address. Link retrieved October 3, 2021.

Keith, J. (2017). *Hooked and booked.* Adactio. Available at https://adactio.com/journal/13109. Link retrieved October 11, 2021.

Kladnik, D. (2021). *I don't care about cookies 3.3.3.* I don't care about cookies. Available at https://www.i-dont-care-about-cookies.eu. Link retrieved October 13, 2021.

Kulyk, O., Hilt, A., Gerber, N., Volkamer, M. (2018). "*This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer.* 3rd European Workshop on Usable Security (EuroUSEC), London, UK. https://doi.org/10.14722/eurousec.2018.23012

Laki sähköisen viestinnän palveluista 2014/917. Available at https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#O7L24P205. Link retrieved October 3, 2021.

Lazarus, R. S., Folkman, S. (1984). *Stress, appraisal, and coping.* New York: Springer.

Leesa-nguansuk, S. (2021). *Controversial law on personal data again postponed, for another year.* Bangkok Post. Available at https://www.bangkokpost.com/business/2110719/controversial-law-on-personal-data-againt-postponed-for-another-year. Link retrieved October 3, 2021.

Maier, M., Harr, R. (2020). *Dark Design Patterns: An End-User Perspective.* Human Technology, Volume 16, Issue 2, Pages 170-199. https://doi.org/10.17011/ht/urn.202008245641

Mathur, A., Acar, G., Friedman, M., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A. (2019). *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites.* Proceedings of the ACM on Human-Computer Interaction, Volume 3, Issue CSCW, Pages 1-32. https://doi.org/10.1145/3359183

Matomo (2021). *Google Analytics alternative that protects your data and your customers' privacy.* Matomo. Available at https://matomo.org. Link retrieved October 3, 2021.

Mauricio Mejía, G. (2021). *Theory-Driven or Theory-Informed? A Review of Behavioural Economics in Design.* The Design Journal, Volume 24, Number 4, Pages 567-587. https://doi.org/10.1080/14606925.2021.1935089

MDN Web Docs (2021a). *Using HTTP cookies.* Mozilla Foundation. Available at https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies. Link retrieved October 3, 2021.

MDN Web Docs (2021b). *Referer.* Mozilla Foundation. Available at https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer. Link retrieved October 3, 2021.

Media Metrics Finland (2021). *Media Site Toplist.* Media Metrics Finland. Available at https://datastudio.google.com/u/0/reporting/445ac769-037b-408e-b383-9014d561cee5/page/QCkcB. Link retrieved October 14, 2021.

Melicher, W., Sharif, M., Tan, J., Bauer, L., Christodorescu, M., Leon, P. (2015). *(Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking.* Proceedings on Privacy Enhancing Technologies, Volume 2016, Issue 2, Pages 135-154. https://doi.org/10.1515/popets-2016-0009

Nouwens, M., Liccardi, I., Veale, M., Karger, D.R., Kagal, L. (2020). *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence.* Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3313831.3376321

noyb (2021). *New browser signal could make cookie banners obsolete.* noyb. https://noyb.eu/en/new-browser-signal-could-make-cookie-banners-obsolete. Link retrieved October 14, 2021.

Office of the Data Protection Ombudsman (2020). *Deputy Data Protection Ombudsman orders company to change the way it requests consent for the use of cookies.* Office of the Data Protection Ombudsman. Available at https://tietosuoja.fi/en/-/deputy-data-protection-ombudsman-orders-company-to-change-the-way-it-requests-consent-for-the-use-of-cookies. Link retrieved October 3, 2021.

Regulation (EU) 2016/679. European Parliament and Council. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN. Link retrieved October 3, 2021.

Rogers, R. W. (1975). *A protection motivation theory of fear appeals and attitude change.* The journal of psychology, Volume 91, Issue 1, Pages 93-114.

Rogers, R. W., Cacioppo, J., Petty, R. (Eds.). (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation.* Social Psychophysiology: A Sourcebook, Pages 153-177. Guilford.

Schmidt, L., Bornschein, R., Maier, E. (2020). *The Effect of Privacy Choice in Cookie Notices on Consumers' Perceived Fairness of Frequent Price Changes.* Psychology and Marketing, Volume 37, Issue 9, Pages 1263-1276. https://doi.org/10.1002/mar.21356

Signal. (2021). *The Instagram ads Facebook won't show you.* Signal Foundation. Available at https://signal.org/blog/the-instagram-ads-you-will-never-see/. Link retrieved October 4, 2021.

Singer, N. (2012). *Mapping, and Sharing, the Consumer Genome.* The New York Times. Available at https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0%20. Link retrieved October 4, 2021.

Soe, T. H., Nordberg, O. N., Guribye, F., Slavkovik, M. (2020). *Circumvention by design - dark patterns in cookie consent for online news outlets.* Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. Association for Computing Machinery, New York, NY, USA, Article 19, Pages 1–12. https://doi.org/10.1145/3419249.3420132

State of California Department of Justice (2018). *California Consumer Privacy Act (CCPA).* State of California. Available at https://oag.ca.gov/privacy/ccpa. Link retrieved October 3, 2021.

Thaler, R. H., Sunstein C. R. (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness.* Yale University Press.

Similarweb (2021). *Top Websites Ranking.* Similarweb. Available at https://www.similarweb.com/top-websites/finland/. Link retrieved October 14, 2021.

Statistics Finland (2016). *National field of education 2016.* Tilastokeskus. Available at https://www.stat.fi/en/luokitukset/koulutusala/koulutusala_1_20160101/. Link retrieved October 14, 2021.

Tolvanen, H. (2021). Correspondence.

Traficom (2019). *Evästeisiin voidaan jatkossakin antaa suostumus selainasetusten kautta.* Liikenne- ja viestintävirasto. Available at https://www.traficom.fi/fi/ajankohtaista/evasteisiin-voidaan-jatkossakin-antaa-suostumus-selainasetusten-kautta. Link retrieved October 3, 2021.

Traficom (2021a). *Hallinto-oikeuden ratkaisut selkeyttivät evästesääntelyn tulkintaa.* Liikenne- ja viestintävirasto. Available at https://www.traficom.fi/fi/ajankohtaista/hallinto-oikeuden-ratkaisut-selkeyttivat-evastesaantelyn-tulkintaa. Link retrieved October 3, 2021.

Traficom (2021b). *Evästeet ja muut käyttäjien päätelaitteille tallennettavat tiedot sekä näiden tietojen käyttö - Opas palveluntarjoajille.* Liikenne- ja viestintävirasto. Available at https://www.traficom.fi/sites/default/files/media/file/Evästeohjeistus_palveluntarjoajille.pdf. Link retrieved October 3, 2021.

Twitter Help (2021). *Our use of cookies and similar technologies.* Built With. Available at https://help.twitter.com/en/rules-and-policies/twitter-cookies. Link retrieved October 3, 2021.

United States Census Bureau (2019). *QuickFacts - California.* U.S. Department of Commerce. Available at https://www.census.gov/quickfacts/CA. Link retrieved October 3, 2021.

Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. (2019). *(Un)informed Consent: Studying GDPR Consent Notices in the Field.* CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications

Security, London, United Kingdom, Pages 973–990. https://doi.org/10.1145/3319535.3354212

Van Bavel, R., Rodriguez-Priego, N. (2016). *Testing the Effect of the Cookie Banners on Behaviour.* Publications Office of the European Union. https://doi.org/10.2791/22197

Vincent, J. (2021). *Facebook bans academics who researched ad transparency and misinformation on Facebook.* The Verge. Available at https://www.theverge.com/2021/8/4/22609020/facebook-bans-academic-researchers-ad-transparency-misinformation-nyu-ad-observatory-plug-in. Link retrieved October 13, 2021.

W3C (2018). *Web Content Accessibility Guidelines (WCAG) 2.1.* World Wide Web Consortium. Available at https://www.w3.org/TR/WCAG21/#requirements-for-wcag-2-1. Link retrieved October 14, 2021.

WebFX (2020). *What Are Data Brokers – And What Is Your Data Worth? [Infographic].* WebFX. Available at https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/. Link retrieved October 4, 2021.

Worldometer (2020). *Thailand Population.* Worldometer. Available at https://www.worldometers.info/world-population/thailand-population/. Link retrieved October 3, 2021.

Xu, H., Dinev, T., Smith, H., Hart, P. (2008). *Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View.* Proceedings of the International Conference on Information Systems, ICIS 2008, Paris, France, Paper 6. http://aisel.aisnet.org/icis2008/6

Zuiderveen Borgesius, F., Poort, J. (2017). *Online Price Discrimination and EU Data Privacy Law.* Journal of Consumer Policy, Issue 40, Pages 347–366. https://doi.org/10.1007/s10603-017-9354-z

APPENDIX A: REVIEWED WEBSITES

Table n. websites and their cookie banner types

Website	Type	Contrast	Characters	Banner type
almamedia.fi	Corporate	FAIL	756	Refusal hidden
ampparit.com	News Portal	FAIL	551	Refusal hidden
areena.yle.fi/tv	Streaming	AAA	316	Refusal hidden
cdon.fi	E-commerce	FAIL	572	Refusal hidden
elisa.fi	ISP	AA	150	Implicit grant
etuovi.com	Marketplace	FAIL	756	Refusal hidden
foreca.fi	Weather	FAIL	1042	Refusal hidden
fortum.fi	Electricity	FAIL	444	Refusal hidden
gigantti.fi	E-commerce	FAIL	356	Refusal hidden
hs.fi	News	FAIL	1096	Refusal hidden
ilmatieteenlaitos.fi	Weather	-	-	-
iltalehti.fi	News	FAIL	756	Refusal hidden
is.fi	News	FAIL	1096	Refusal hidden
k-ruoka.fi	E-commerce	FAIL	276	Refusal hidden
karkkainen.com	E-commerce	FAIL	205	Refusal hidden
kauppalehti.fi	News	FAIL	756	Refusal hidden
kela.fi	Government	AA	341	Neutral banner
kone.fi	Corporate	FAIL	208	Refusal hidden
motonet.fi	E-commerce	AA	150	Implicit grant
mtvuutiset.fi	News	FAIL	1356	Refusal hidden
neste.fi	Corporate	FAIL	289	Refusal hidden
netrauta.fi	E-commerce	FAIL	158	Implicit grant
nettiauto.com	Marketplace	FAIL	511	Refusal hidden
nettix.fi	Corporate	FAIL	298	Refusal hidden
nokia.com/fi_fi	Telecom	AAA	218	Neutral banner
nordea.fi	Banking	AAA	837	Refusal hidden

Website	Type	Contrast	Characters	Banner type
oikotie.fi	Marketplace	FAIL	1066	Refusal hidden
op.fi	Banking	FAIL	414	Neutral banner
orion.fi	Corporate	FAIL	801	Neutral banner
pitkospuu.fi	Ad Agency	FAIL	105	Neutral banner
pixels.fi/fi/	Ad Agency	FAIL	210	Refusal hidden
posti.fi	Postal Service	FAIL	585	Refusal hidden
power.fi	E-commerce	FAIL	312	Refusal hidden
redland.fi	Ad Agency	FAIL	688	Refusal hidden
sampo.com/fi/	Corporate	FAIL	221	Implicit grant
seiska.fi	Tabloid	FAIL	1072	Refusal hidden
storaenso.com/fi-FI	Corporate	FAIL	289	Refusal hidden
suomi.fi	Government	-	-	-
suomi24.fi	Forum	FAIL	808	Refusal hidden
taloon.fi	E-commerce	FAIL	169	Implicit grant
talouselama.fi	News	FAIL	756	Refusal hidden
telia.fi	ISP	FAIL	479	Refusal hidden
tori.fi	Marketplace	FAIL	1063	Refusal hidden
tulos.fi	Ad Agency	FAIL	254	Neutral banner
upm.com/fi/	Corporate	FAIL	275	Refusal hidden
veikkaus.fi	Gambling	AAA	363	Implicit grant
verkkokauppa.com	E-commerce	FAIL	173	Implicit grant
yle.fi	News	AAA	316	Refusal hidden
ylilauta.org	Forum	-	-	-
zalando.fi	E-commerce	FAIL	884	Refusal hidden

APPENDIX B: COOKIE BANNER TEXTS

Encouraging

Evästeet ovat pieniä tekstitiedostoja, jotka tallennetaan tietokoneellesi. Voit halutessasi poistaa evästeet selaimen asetuksista.

Käytämme evästeitä kerätäksemme anonymisoituja tilastotietoja sivuston kävijöistä. Tietoa käytetään ainoastaan sivuston käyttäjäkokemuksen parantamiseen sekä teknisten vikojen havaitsemiseen ja diagnosointiin. Hyväksymällä evästeet autat meitä tekemään sivustostamme toimivamman. Tietoja ei käytetä esimerkiksi mainonnan kohdentamiseen emmekä koskaan luovuta tietoja kolmansille osapuolille.

Voit antaa suostumuksesi painamalla "Hyväksy kaikki”.

Discouraging

Evästeet ovat pieniä tekstitiedostoja, jotka tallennetaan tietokoneellesi. Voit halutessasi poistaa evästeet selaimen asetuksista.

Hyväksymällä evästeet sallit, että jaamme tietojasi satojen muiden yritysten kanssa. Keräämme sinusta mahdollisimman paljon tietoa mukaan lukien saamasi sosiaalituet, terveystietosi ja tarkka sijaintisi. Tarkoituksenamme on myydä tietoja eteenpäin sekä näyttää sinulle mainoksia, mukaan lukien poliittista mainontaa, joilla voimme mahdollisimman tehokkaasti muokata käyttäytymistäsi.

Voit antaa suostumuksesi painamalla "Hyväksy kaikki”.

APPENDIX C: ORIGINAL QUESTIONNAIRES

Kyselylomake

Tämä on ensimmäinen tutkimuksen kolmesta kyselystä, ja tässä kysytään muutamia perustietoja yleisellä tasolla.

Ikäsi vuosina

Sukupuoli

- Mies
- Nainen
- Muu
- En halua sanoa

Korkein suorittamasi koulutustaso

- Peruskoulu
- Lukio tai ammattikoulutus
- Alempi korkeakoulututkinto
- Ylempi korkeakoulututkinto
- Lisensiaatin tai tohtorintutkinto
- Muu koulutustaso

Työ- ja opiskelutilanteesi

- Opiskelija
- Työssäkäyvä
- Yrittäjä
- Työtön
- Eläkkeellä
- Muu työllisyystilanne

Koulutusalasi

- Yleissivistävä koulutus
- Kasvatusalat
- Humanistiset ja taidealat
- Yhteiskunnalliset alat
- Kauppa, hallinto ja oikeustieteet
- Luonnontieteet
- Tietojenkäsittely ja tietoliikenne (ICT)
- Tekniikan alat
- Maa- ja metsätalousalat
- Terveys- ja hyvinvointialat
- Palvelualat
- Muu koulutusala

Lähetä ja jatka

Tietotekniikkataitojen arviointi

Tämä on toinen tutkimuksen kolmesta kyselystä. Kyseessä on tietotekniikkataitojen itsearviointi, ja siinä on yhteensä kaksitoista väittämää.

Valitse vaihtoehto väliltä 1-7 riippuen siitä, kuinka samaa mieltä olet väittämän kanssa (1 = täysin eri mieltä, 4 = en eri enkä samaa mieltä, 7 = täysin samaa mieltä). Vastaa kaikkiin väittämiin.

1. Osaan aina ratkaista vaikeatkin tietokoneisiin liittyvät ongelmat kunhan vain yritän riittävästi.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

2. Jos tietokoneeni temppuilee, löydän tavan jolla saan sen toimimaan kuten haluan.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

3. Minun on helppo saavuttaa tietotekniikan käyttöön liittyvät tavoitteeni.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

4. Luotan siihen, että osaan hoitaa tehokkaasti tietokoneisiin liittyvät odottamattomat tilanteet.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

5. Opin käyttämään useimpia tietokoneohjelmistoja, jos vain näen riittävästi vaivaa asian eteen.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

6. Pysyn rauhallisena kohdatessani tietoteknisiä vaikeuksia, koska voin luottaa omiin kykyihini ratkaista ne.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

7. Kun kohtaan tietoteknisen ongelman, löydän useimmiten useita ratkaisuja ongelmaan.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

8. Osaan useimmiten hoitaa kohtaamani tietotekniset ongelmat.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

9. Jos en onnistu tekemään tietokoneella jotain, se saa minut yrittämään kovemmin.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

10. Koen olevani itsenäinen ja pystyvä kun on kyse tietokoneella tehtävistä asioista.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

11. On vain vähän asioita, joita en osaa tehdä tietokoneella.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

12. Voin sinnikkäästi yrittämällä suorittaa melkein minkä tahansa tietokoneisiin liittyvän tehtävän.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

Lähetä ja jatka

Loppukysely

Onnittelut, olet melkein valmis! Tässä on vielä muutama kysymys.

1. Testisivusto esitti sinulle evästebannerin, jossa sinulla oli mahdollisuus joko hyväksyä evästeiden käyttö tai kieltäytyä evästeistä. Päätit kieltäytyä evästeistä. Miksi toimit näin? Valitse kaikki väittämät, joiden kanssa olet samaa mieltä.

- [ ] Kieltäydyin tietosuojasyistä
- [ ] Oletin, että evästeiden salliminen voisi altistaa minut haittaohjelmille
- [ ] En koe, että hyväksyminen olisi hyödyttänyt minua itseäni
- [ ] Minulle ei ole väliä sillä, käyttääkö sivusto evästeitä vai ei
- [ ] En osaa sanoa
- [ ] Muu syy

2. Jos vastasit edelliseen kysymykseen "Muu syy" tai haluat muuten vain perustella valintojasi, kirjoita perustelusi tähän.

3. Oletetaan, että selaimessasi olisi asetus, jolla voit yhdellä klikkauksella joko kieltää tai sallia kaikki paitsi teknisesti välttämättömät evästeet kaikilla sivustoilla. Valittuasi kumman tahansa vaihtoehdoista et näe enää evästebannereita millään sivustolla. Kaikki sivustot myös toimivat samalla tavalla riippumatta siitä, kumman vaihtoehdon valitset.

Jos tällainen asetus olisi olemassa, kumman vaihtoehdon valitsisit?

- ( ) Hyväksyn kaikki evästeet
- ( ) Hylkään kaikki evästeet (paitsi teknisesti välttämättömät)
- ( ) En osaa sanoa

Lähetä

Loppukysely

Onnittelut, olet melkein valmis! Tässä on vielä muutama kysymys.

1. Testisivusto esitti sinulle evästebannerin, jossa sinulla oli mahdollisuus joko hyväksyä evästeiden käyttö tai kieltäytyä evästeistä. Päätit hyväksyä evästeet. Miksi toimit näin? Valitse kaikki väittämät, joiden kanssa olet samaa mieltä.

- [ ] Haluan nähdä itselleni räätälöityjä mainoksia tai sisältöä
- [ ] Evästeiden hyväksyminen auttaa parantamaan sivuston laatua
- [ ] Oletin, että sivustoa ei voi käyttää lainkaan hyväksymättä evästeitä
- [ ] Oletin sivuston toimivan huonommin jos evästeitä ei hyväksy
- [ ] Oletin, että kieltäytyminen olisi vaikeampaa kuin hyväksyminen
- [ ] Oletin sivuston käyttävän evästeitä joka tapauksessa
- [ ] Minulle ei ole väliä sillä, käyttääkö sivusto evästeitä vai ei
- [ ] En osaa sanoa
- [ ] Muu syy

2. Jos vastasit edelliseen kysymykseen "Muu syy" tai haluat muuten vain perustella valintojasi, kirjoita perustelusi tähän.

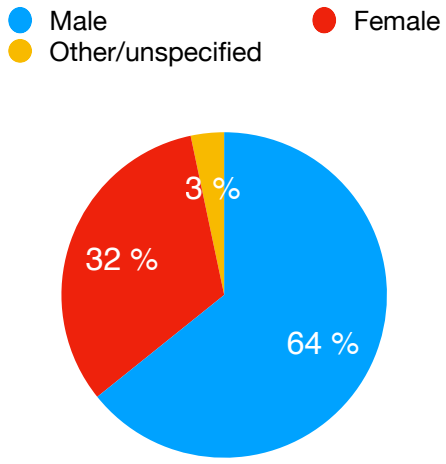
3. Oletetaan, että selaimessasi olisi asetus, jolla voit yhdellä klikkauksella joko kieltää tai sallia kaikki paitsi teknisesti välttämättömät evästeet kaikilla sivustoilla. Valittuasi kumman tahansa vaihtoehdoista et näe enää evästebannereita millään sivustolla. Kaikki sivustot myös toimivat samalla tavalla riippumatta siitä, kumman vaihtoehdon valitset.

Jos tällainen asetus olisi olemassa, kumman vaihtoehdon valitsisit?

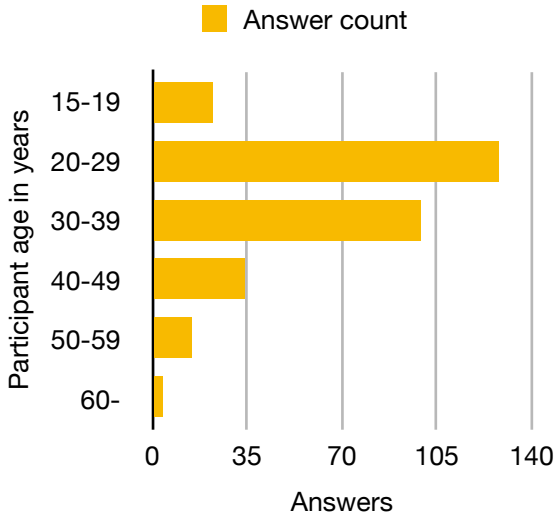
- ( ) Hyväksyn kaikki evästeet
- ( ) Hylkään kaikki evästeet (paitsi teknisesti välttämättömät)
- ( ) En osaa sanoa

Lähetä

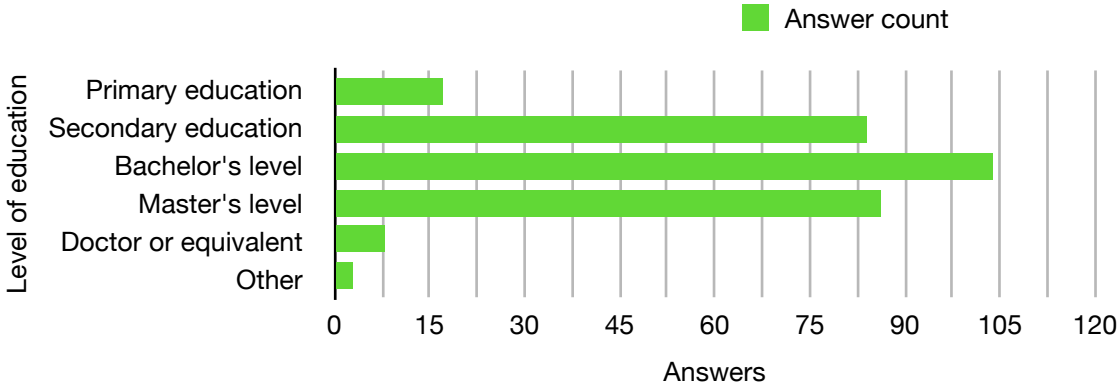
APPENDIX D: DEMOGRAPHIC DATA



Answers by gender. (All participants)



Answers by age group. (All participants)



Answers by age group. (All participants)

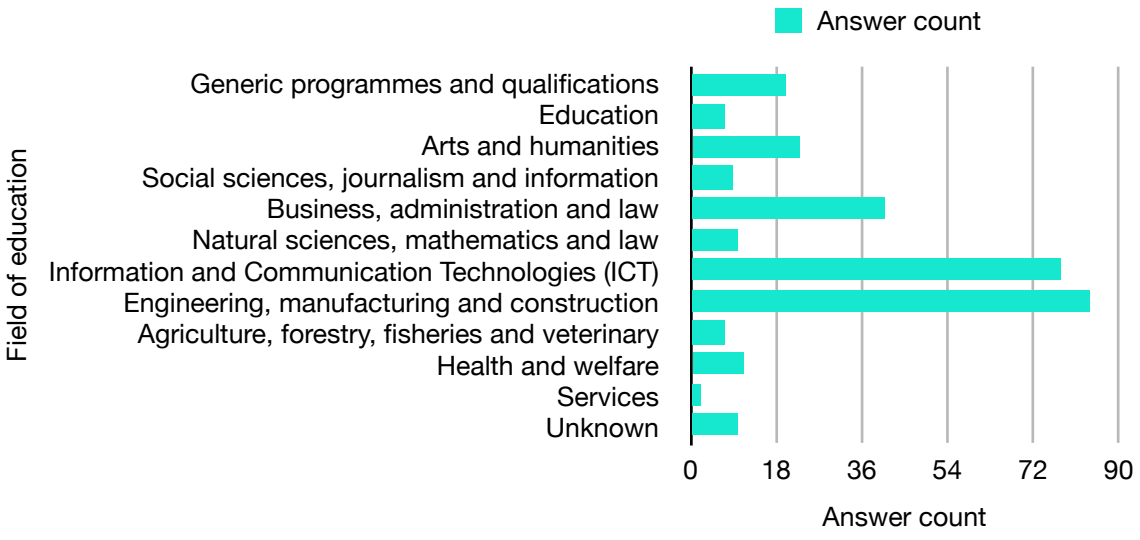
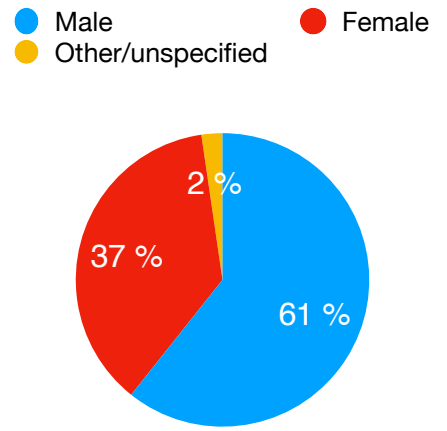
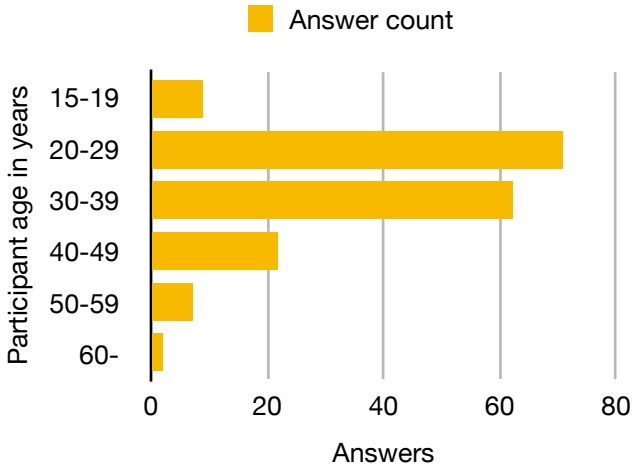


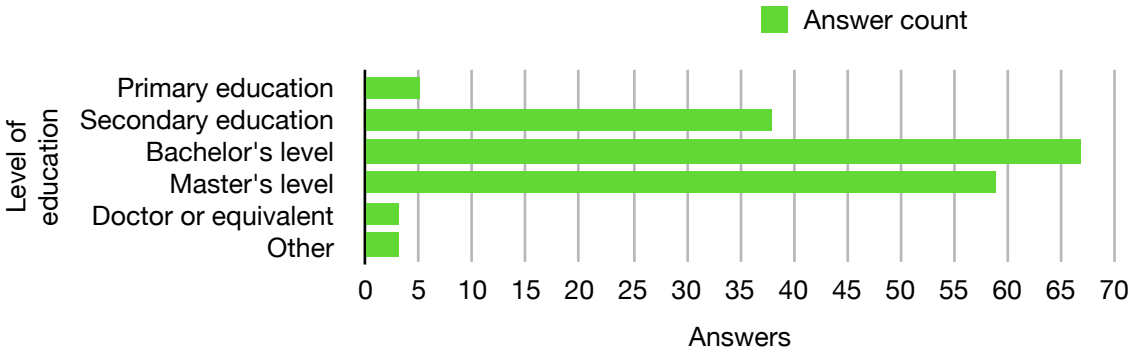
Figure n. Answers by field of education. (All participants)



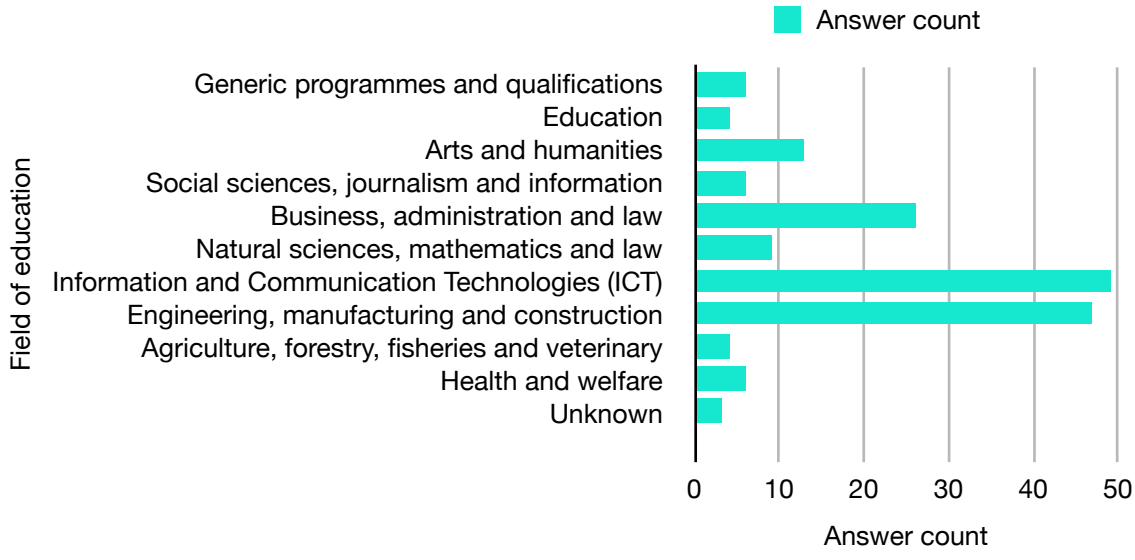
Answers by gender. (Motivation questionnaire)



Answers by age group. (Motivation questionnaire)



Answers by age group. (Motivation questionnaire)



Answers by field of education. (Motivation questionnaire)