

Noora Tuokkola

**USERS' PERCEPTIONS OF PRIVACY IN COOKIE
CONSENT REQUESTS WITH DECEPTIVE DESIGN**



UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2024

ABSTRACT

Tuokkola, Noora

Users' perceptions of privacy in cookie consent requests with deceptive design
Jyväskylä: University of Jyväskylä, 2024, 121 pp.

Information Systems, Master's Thesis

Supervisor: Koskelainen, Tiina

This master's thesis contributed to the growing need to understand and protect users' privacy as deceptive design practices (also known as dark patterns) have become more prevalent and are now commonly found in cookie consent requests, which have an important role in users' ability to control their privacy. To address this issue, and fill a gap in literature, the study looked at how users perceive their privacy in cookie consent requests that include deceptive patterns, and what the role of deceptive design is in this perception. A theoretical framework for understanding users' perceptions of privacy, as inspired by previous models of perceived privacy, was proposed, consisting of four influencing factors that were used as guiding themes throughout the study: privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks. The study was conducted with method triangulation, combining user testing, a think-aloud method, and thematic interviews to comprehensively capture users' perceptions. The study uniquely took a qualitative, user experience-oriented perspective on the topic, addressing deceptive design's role in the perception. The findings revealed that deceptive design diminishes users' perceived control over their privacy and their trust in the cookie data collector, while its influence on users' privacy concerns and perceived privacy risks is more subtle and varied. Although users may have learned to withstand or bypass deceptive design due to its ubiquity, the overarching theme was its negative influence on privacy perceptions. Users' overall perceptions of privacy in cookie consent requests were fluid, influenced by design, context, and users' habits and interest in privacy protection. Even though the findings cannot be concluded into one general perception, the findings lean toward users perceiving their privacy as compromised, undervalued, and unprotected. The findings of this study, combined with findings from previous research and legislative measures, all ultimately emphasize the need to discontinue using deceptive design and commit to privacy-protective design guidelines.

Keywords: deceptive design, deceptive patterns, dark patterns, cookies, cookie consent requests, privacy, perception of privacy, privacy by design

TIIVISTELMÄ

Tuokkola, Noora

Käyttäjien havaintoja yksityisyydestä harhaanjohtavissa evästepyyntöissä

Jyväskylä: Jyväskylän yliopisto, 2024, 121 s.

Tietojärjestelmätiede, pro gradu -tutkielma

Ohjaaja: Koskelainen, Tiina

Tämä pro gradu -tutkielma vastasi kasvavaan tarpeeseen ymmärtää ja suojella käyttäjien yksityisyyttä harhaanjohtavien muotoilukeinojen (tunnetaan myös nimillä pimeät käytännöt ja synkät suunnittelumallit) käytön lisääntyessä etenkin evästepyyntöissä, joilla on merkittävä rooli käyttäjien mahdollisuuksiin kontrolloida yksityisyyttään. Tutkimuksessa selvitettiin, millaiseksi käyttäjät havaitsevat yksityisyytensä sellaisissa evästepyyntöissä, joissa on käytetty harhaanjohtavaa muotoilua. Lisäksi tutkittiin, millainen vaikutus harhaanjohtavalla muotoilulla on näihin havaintoihin. Aiempien tutkimusmallien pohjalta tutkimusta varten luotiin teoreettinen viitekehys ymmärtämään käyttäjien yksityisyyden havaintoja. Viitekehys koostui neljästä vaikuttavasta tekijästä, jotka toimivat ohjaavina teemoina läpi tutkimuksen: yksityisyyden huolet, kontrolli omasta yksityisyydestä, luottamus (eväste)tietojen kerääjää kohtaan ja havaitut riskit yksityisyydelle. Tutkimus toteutettiin menetelmätriangulaationa yhdistelmällä käyttäjätestausta, ääneenajattelua ja puolistrukturoitua teemahaastattelua, jotta saataisiin mahdollisimman kokonaisvaltainen ymmärrys käyttäjien havainnoista. Tulokset osoittivat, että harhaanjohtava muotoilu heikensi käyttäjien havaitsemaa kontrollia yksityisyydestään sekä luottamusta evästetietojen kerääjää kohtaan. Vaikutus havaittuihin yksityisyyden huoliin ja riskeihin oli vähäisempi ja vaihtelevampi. Vaikka käyttäjät ovat saattaneet tottua sietämään ja sivuuttamaan harhaanjohtavaa muotoilua, niin pääasiallisesti tulokset kuitenkin osoittivat harhaanjohtavan muotoilun negatiivisen vaikutuksen käyttäjien havaintoihin yksityisyydestään. Tulokset käyttäjien yksityisyyden kokonaishavainnoista harhaanjohtavissa evästepyyntöissä vaihtelivat riippuen muotoilukeinosta ja kontekstista sekä käyttäjien totumuksista ja kiinnostuksesta omaa yksityisyydensuojaa kohtaan. Siitä huolimatta tulokset kuitenkin viittasivat eniten siihen, että yksityisyys koettiin vaarantuneeksi, aliarvostetuksi ja suojattomaksi. Tulokset yhdessä aiemman tutkimuksen ja lainsäädännön kanssa korostavat tarvetta lopettaa harhaanjohtavan muotoilun käyttö ja sitoutua sisäänrakennetun yksityisyydensuojan muotoiluperaatteisiin.

Asiasanat: harhaanjohtava muotoilu, pimeät käytännöt, synkät suunnittelumallit, evästeet, evästepyyntöt, yksityisyys, yksityisyyden havainnot, sisäänrakennettu yksityisyydensuoja

FIGURES

FIGURE 1 The study's theoretical framework for the perception of privacy	29
FIGURE 2 The first cookie consent request mock-up used in user testing	49
FIGURE 3 The second cookie consent request mock-up used in user testing	50
FIGURE 4 The third cookie consent request mock-up used in user testing	51

TABLES

TABLE 1 Deceptive patterns commonly found in cookie consent requests, with examples	17
TABLE 2 Users' perceptions of privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks in cookie consent requests without and with deceptive design	71

TABLE OF CONTENTS

ABSTRACT

TIIVISTELMÄ

FIGURES AND TABLES

1	INTRODUCTION	8
2	COOKIES AND DECEPTIVE DESIGN.....	11
2.1	Cookies and cookie consent requests.....	11
2.1.1	Cookies.....	11
2.1.2	Cookie compliance: GDPR, ePrivacy, and beyond	12
2.1.3	Cookie consent requests	13
2.1.4	Previous research on users' perceptions of cookie consent requests	14
2.2	Deceptive design and deceptive patterns	15
2.2.1	Deceptive design elements: deceptive patterns.....	15
2.2.2	Types of deceptive patterns	16
2.2.3	Legislation prohibiting deceptive design	18
2.2.4	Previous research on users' perceptions of deceptive design ...	18
3	PRIVACY AND DESIGN.....	21
3.1	Introduction to privacy concepts and definitions.....	21
3.1.1	Evolution of privacy: historical context	21
3.1.2	Evolution of privacy: the digital era.....	23
3.2	Privacy-protective design.....	24
4	THEORETICAL FRAMEWORK FOR THE PERCEPTION OF PRIVACY.....	28
4.1	Overview of the framework	28
4.2	Previous models inspiring this framework.....	30
4.3	Influencing factors within the framework	33
4.3.1	Privacy concerns.....	34
4.3.2	Control over privacy	35
4.3.3	Trust in the (cookie) data collector	37
4.3.4	Perceived privacy risks.....	38
4.4	Design's role in the framework	39
4.5	Previous research on users' perceptions of privacy in cookie consent requests and deceptive design.....	40
4.5.1	Perceptions of privacy concerns.....	40
4.5.2	Perceptions of control	40
4.5.3	Perceptions of trust	41
4.5.4	Perceptions of privacy risks.....	42
5	RESEARCH METHODOLOGY	43

5.1	Triangulation of research methods: user testing, think-aloud, and thematic interviews	43
5.2	Conducting the study.....	46
5.2.1	Participants and recruitment	46
5.2.2	Creating mock-ups for user testing	48
5.2.3	Conducting user testing with the think-aloud method	52
5.2.4	Conducting thematic interviews.....	52
5.3	Data analysis.....	54
5.3.1	Data overview	54
5.3.2	Analysis process	55
5.4	Ethical and privacy considerations	57
5.5	Trustworthiness and methodological limitations	59
5.6	Use of artificial intelligence in this thesis	61
6	RESULTS	63
6.1	Deceptive design's influence on users' privacy concerns, control over privacy, trust, and perceived privacy risks.....	63
6.1.1	Privacy concerns.....	63
6.1.2	Control over privacy	65
6.1.3	Trust in the cookie data collector	67
6.1.4	Perceived privacy risks.....	68
6.2	Additional findings influencing the perception of privacy.....	71
6.2.1	User's personal interest	72
6.2.2	Importance of deceptive design's influence in comparison to other factors.....	72
6.2.3	Privacy attributes and design-specificity.....	73
6.2.4	Ubiquity and avoidance of the topic	74
6.3	Users' impressions of deceptive design and cookies	75
6.3.1	Emotions and cognitive states regarding deceptive design in cookie consent requests	75
6.3.2	Descriptions of deceptive design in cookie consent requests....	76
6.3.3	Descriptions of cookie data collectors	78
7	DISCUSSION	79
7.1	Deceptive design's influence on users' perceptions of privacy in cookie consent requests.....	79
7.1.1	Influence on users' privacy concerns	80
7.1.2	Influence on users' control over privacy	81
7.1.3	Influence on users' trust in the cookie data collector.....	82
7.1.4	Influence on users' perceived privacy risks	83
7.1.5	Other key findings regarding deceptive design's influence	84
7.1.6	Concluding remarks on deceptive design's influence on the perceptions of privacy	85
7.2	Users' overall perceptions of privacy in cookie consent requests that include deceptive design	86

7.2.1	Perceptions of privacy: control.....	86
7.2.2	Perceptions of privacy: trust and transparency issues	87
7.2.3	Perceptions of privacy: privacy concerns and risks	87
7.2.4	Perceptions of privacy: users' descriptions and reactions to deceptive design in cookie consent requests.....	88
7.2.5	Conclusion on users' overall perceptions of privacy	89
7.3	Concluding summary of key findings	90
7.4	Contributions to theory and practice.....	91
7.4.1	Theoretical contributions	91
7.4.2	Practical contributions	92
7.5	Limitations of the study	93
7.6	Suggestions for future research	94
8	CONCLUSIONS	96
	REFERENCES.....	99
	APPENDIX 1 OUTLINE FOR USER TESTING AND INTERVIEWS.....	108
	APPENDIX 2 MOCK-UPS FOR USER TESTING	113
	APPENDIX 3 INFORMATION LEAFLET FOR PARTICIPANTS	116
	APPENDIX 4 PRIVACY NOTICE FOR PARTICIPANTS	119

1 INTRODUCTION

Due to legislative changes, especially the introduction of the General Data Protection Regulation (GDPR; Regulation (EU) 2016/679) in 2016, user's permission is now required for collecting and using *cookies* on any website in the European Union. Therefore, the user is presented with a *cookie consent request* when first entering a website. The ubiquity of these requests has caused users to experience something called "cookie blindness", which causes them to habitually give their consent without reading the content of the request (Mejtoft et al., 2021). Additionally, the frequent encounters with these requests are causing the users to develop negative emotions around them (e.g., Ha et al., 2006; Habib et al., 2019; Kulyk, Hilt, Gerber, & Volkamer, 2018; Mejtoft et al., 2023; Nouwens et al., 2020) as well as seeing them as overly intrusive (Ha et al., 2006), ultimately making the users unsatisfied with the requests (Utz et al., 2019).

As cookie consent requests have become a daily occurrence to users, so have *deceptive design* elements, such as *deceptive patterns* (Di Geronimo et al., 2020; Lupiáñez-Villanueva et al., 2022). Deceptive patterns - often known as dark patterns, those misleading interface elements - are used to direct users into accepting more cookies than they originally intended (Brignull et al., 2023). Deceptive patterns are used, as they can increase the company's conversion rates (Brignull, 2011). On the contrary, the company might not be intentionally using deceptive design as they might get their cookie consent request designs directly from consent management platforms (CMPs) that offer pre-made request interface designs (see e.g., Nouwens et al., 2020). No matter the reason behind companies using deceptive patterns in their cookie consent requests, their existence is prominent. For example, Utz et al. (2019) found that a minimum of 57,4% of the 1000 CMPs selected for their study used deceptive patterns that nudged users toward a privacy-unfriendly option. Similarly, Alharbi et al. (2023) found that more than 90% of the cookie consent requests selected for their study had deceptive patterns. Additionally, Krisam et al. (2021) also noticed in their study of 500 German websites' cookie consent requests that 85% of them directed users to accepting all cookies.

The current study is important for a multitude of reasons but most importantly it has to do with protecting users' privacy. Cookie consent requests

play an important role in a user's ability to control their own privacy (what and how much data is collected of them) and therefore the requests should, by law, contain sufficient and clear information about the use of collected information and its effect on the user's privacy (GDPR, 2016/679). Deceptive patterns attempt to hide and disguise this information and make it seem like consenting to all cookies' collection would be the best choice for the user, even though it is in fact the least privacy-protective option (Mathur et al., 2021). Despite regulation, deceptive patterns are still used, and literature shows that privacy regulations are not always followed. For example, in a study by Alharbi et al. (2023), nearly 70% out of the 243 websites' cookie consent requests that they studied violated at least one privacy guideline. While cookies can improve a website's functionality and user experience, unintentionally sharing excess cookie data because of deceptive patterns can oppose threats to the user's privacy (Alharbi et al., 2023). Multiple scholars, such as Habib et al. (2019), Mathur et al. (2021), and Utz et al. (2019) have reported that deceptive patterns undermine and diminish users' privacy, as they influence the user's own freedom of choice and control.

Despite multiple researchers' (including Machuletz & Böhme, 2020; Nouwens et al., 2020) attempts to point out deceptive design's negative influence on users' privacy, actions toward getting these findings to better contribute to practice are still required. The literature on cookie consent requests is constantly growing, possibly due to users' consent being collected in privacy-threatening ways (Alharbi et al., 2023), and there being the need to make a change in design and development practices to change this current state. There have been efforts to make cookie consent requests' design more privacy-protective (e.g., Kulyk, Mayer, Käfer, & Volkamer, 2018), as well as creating guidelines for privacy-protective design (for example, Privacy by Design principles by Cavoukian, 2010; Privacy Attributes by Barth et al., 2022). Still, the need for establishing these guidelines and more broadly regulating the use of deceptive design is apparent in order to reliably assure users' privacy.

Previous research has predominantly used quantitative methods to address users' behavior regarding consent-choices, prevalence of deceptive design, as well as legislative compliance of cookie consent requests. While there is some research on users' perceptions, emotions and impressions on both deceptive design (e.g., Bongard-Blanchy et al., 2021; Di Geronimo et al., 2020; Maier & Harr, 2020) and cookie consent requests (e.g., Ha et al., 2006; Kulyk, Hilt, Gerber, Volkamer, 2018), there is only little qualitative, user experience-oriented research on how users perceive their privacy within this context (e.g., Mejtoft et al., 2023). There is a notable gap in qualitative studies addressing how users overall perceive their privacy when interacting with deceptively designed cookie consent requests, and especially, what is design's role in this perception.

While previous studies (such as, Adams, 1999; Chang et al., 2018; Dinev et al., 2013) have studied *perceived privacy*, this study attempts to make a difference between perceived privacy - measurable, rational, and often static concept - and the *perception of privacy* - fluid, subjective user experience. In this study, a theoretical framework for the users' perception of privacy is proposed (as inspired by

the models of Adams, 1999; Chang et al., 2018; Dinev et al., 2013), consisting of four influencing factors: privacy concerns, control over privacy, trust, and perceived privacy risks. These influencing factors are used as guiding themes, not as measurable variables, throughout the study. The study investigates how design, more specifically deceptive design, influences users' overall perceptions of privacy and the four influencing factors within. Previous studies (Adams, 1999; Lai, 2016; San Martín & Camarero, 2009) have shown signs of the connection between design and perception privacy although their direct connection is not yet confirmed. Despite previous research delving into users' perceptions of deceptive design and cookie consent requests, as well as individually focusing on users' perceptions on the four influencing factors, no prior research has qualitatively looked at how the factors contribute to the overall, user experience-oriented, perception of privacy, and what kind of role deceptive design has in shaping the perception.

In this study, a qualitative, triangulated approach is taken, combining user testing, a think-aloud method, and thematic interviews to comprehensively capture users' perceptions of privacy. This combination of methods allows for rich data collection, adding to the depth and trustworthiness of the study. Answers to the following research questions are looked for, guided by the theoretical framework and other supporting theories:

Q1 How does deceptive design influence users' perceptions of privacy in cookie consent requests?

Q2 What are users' overall perceptions of privacy in cookie consent requests that include deceptive patterns?

Ultimately, this study contributes to the growing body of literature on understanding and protecting users' privacy as deceptive design practices become more prevalent. The findings offer a novel idea to the literature, suggesting that users' perceptions of privacy are a fluid and subjective user experience rather than a static, rational, and measurable concept. Additionally, deceptive design's role in the perception is highlighted. Most importantly, this study advocates for honest, ethical, and transparent design practices to improve users' perceptions of privacy, supporting the adherence to privacy-protective design guidelines.

The structure of this thesis is as follows. Chapter 2 introduces key concepts, including cookies, cookie consent requests, deceptive design, and deceptive patterns. Chapter 3 defines privacy and presents privacy-protective design frameworks. Chapter 4 introduces the theoretical framework for the perception of privacy used in this study, including the four influencing factors and the role of design in it. Chapters 2 to 4 also introduce relevant previous research. Chapter 5 explains the study's methodology, data collection, and data analysis process. Chapter 6 presents the study's results, while chapter 7 answers the research questions, discusses the findings in light of prior research, addresses the study's limitations and contributions, and gives suggestions for future research. Finally, the conclusions chapter summarizes the main points of the study.

2 COOKIES AND DECEPTIVE DESIGN

In this chapter, the following key concepts are introduced: cookies, cookie consent requests, deceptive design, and deceptive patterns. After introducing each concept, previous research regarding users' perceptions of it are presented. Additionally, relevant legislation related to cookies, user's consent, and deceptive design in the European Union and Finland are introduced.

2.1 Cookies and cookie consent requests

In this section, cookies, and later, cookie consent requests are defined. Additionally, their legislative compliance is considered. Lastly, previous research regarding users' perceptions of cookies is presented.

2.1.1 Cookies

Cookies, also known as HTTP- or web cookies, were first introduced in 1994, and are small text files that websites store on users' browsers to track users' interactions and preferences (Kristol, 2001). Cookies have various purposes, such as improving the functionality of the website, improving security and privacy, gathering data on how the site is used, and making the site better suitable for users' interests (Finnish National Cyber Security Center [Traficom], n.d.). Cookies are either session-based, disappearing after a single visit to the website, or permanent, stored on the user's device until manually deleted or expired (Traficom, n.d.).

Cookies are broadly categorized based on their purpose. Essential, or functional, cookies have a direct effect on the functionality of the website, and it is not necessary to, by law, ask for the user's consent to use them, although it is recommended to inform them as a fair practice (Kretschmer et al., 2021; Traficom, n.d.). Non-essential, or non-functional, cookies - like those for analytics, marketing, and personalization - collect personally identifiable user data beyond just the basic functionality of the website (Kretschmer et al., 2021). The non-essential

cookies mainly improve the user's experience or improve the website's conversion rates or performance (Traficom, n.d.). Additionally, cookies can be categorized based on their origin: first-party cookies are set by the visited website, while third-party cookies are often used by external entities (Kretschmer et al., 2021; Traficom, n.d.), such as Meta or Google.

This variation in cookies' functionality, purpose and origin has made users' consent a critical aspect of protecting their data privacy (Kretschmer et al., 2021). This has driven policymakers to develop legislation for protecting users from involuntary data collection, as introduced in the following subsections.

2.1.2 Cookie compliance: GDPR, ePrivacy, and beyond

As shortly mentioned previously, cookie data collection is regulated by legislation. This subsection introduces the main legislations regarding cookies both in the European Union and Finland.

In the European Union, two of the most important legislations are The General Data Protection Regulation (GDPR; 2016/679), and the Directive on Privacy and Electronic Communications (ePrivacy Directive; 2002/58/EC). The GDPR (Regulation 2016/679) became effective in May 2018, making cookie consent requests besides many other data protection measures mandatory, and allowing users to finally be in charge of their personal data collection online. The ePrivacy Directive (2002/58/EC) contains rules and guidelines for the processing of personal data and the protection of privacy in the electronic communications sector, including themes around confidentiality, and rules regarding tracking and monitoring. The ePrivacy Directive has in some cases been called as the "cookie law", due to it having the most legislative content over cookie collection and use in the European Union (Koch, 2019). The ePrivacy Directive (2002/58/EC, Article 5(3), Recitals 24 and 25) recognizes both the importance and usefulness of cookies to modern online services as well as threats that they oppose to users' privacy. Additionally, the European Electronic Communications Code (Directive 2018/1972) provides legislation related to the users' rights in electronic communications networks and services.

In Finland, there are also national legislative acts when it comes to users' online privacy and cookies. The most significant one being the Act on Electronic Communications Services (Act 917/2014, 2023, Section 205), which regulates the storage and collection of cookies in online services in Finland.

Despite legislation's importance and impact, researchers such as Liu et al. (2022) have questioned whether the current legislation is in fact effectively protecting users' online privacy. To support this, Matte et al. (2020) extensively studied cookie consent requests on 560 websites and detected more than 50% of them to have at least one legislation violation related to the GDPR regulation or the ePrivacy directive. As the legislation is still relatively young, these kinds of findings may be expected, as not every practitioner is yet familiar with them.

2.1.3 Cookie consent requests

Due to legislative changes, as presented in the previous subsection, user's permission is now required for collecting and using non-essential cookies on any website in the EU. Therefore, the user is presented with a *cookie consent request* (also commonly known as cookie banner or consent notice; later also referred to as consent requests or requests) when first entering a website.

A cookie consent request's purpose is to inform the user about cookie collection's purpose, storage, and use, and to get the user's informed consent for collecting them in the first place (Finnish Transport and Communications Agency [Traficom], 2022). Another important reason for the request is to make the user more aware of their privacy and the company's privacy practices (Traficom, 2022). By law (GDPR, 2016/679), the request should include an accurate and specific description of what type of data is collected of the user, why, and for how long the cookie data will be saved for, who is responsible for storing it and where. The request should also inform whether third parties are going to have access to the cookie data, and a good practice would be to offer options for the user to not only opt-in or opt-out their consent, but also to select which types of cookies they want to consent to (Traficom, 2022). Additionally, the request must now feature a simple option for rejecting the collection of all non-essential cookies (Traficom, 2022), and to comply with the GDPR (Regulation 2016/679), the user should be able to withdraw their consent as easily as it was given, for example, by providing access to cookie settings on the website's menu. For the user to be able to edit their consent later, the GDPR (Regulation 2016/679), requires for the website to document and store the user's consent decision. Lastly, the GDPR (Regulation 2016/679) demands that the user should be able to access the website even without consenting to non-essential cookies.

A cookie consent request is commonly presented as a dialogue box (a banner) that floats over the content of the website (Alharbi et al., 2023). The request normally involves two to three consent options for the user to choose from: accept, decline, and manage options (Alharbi et al., 2023; Kretschmer et al., 2021; Singh et al., 2022). Sometimes, the user can also find an option to click "accept only essential cookies" (Alharbi et al., 2023), or it might be possible to click the X in the corner of the request to exit it. Alharbi et al. (2023), Kretschmer et al. (2021), and Singh et al. (2022) all have studied the prevalence of different consent request styles, resulting in the following two styles being the most common: binary options (opt-in or opt-out consent), and cookie categories (multiple cookie category types to choose from for the consent). Singh et al. (2022) and Kretschmer et al. (2021) found that a style that offers the user categories to choose from is best in line with user privacy, as it gives the user the most control over the consent choice. Additionally, Alharbi et al. (2023) and Kretschmer et al. (2021) found an informational cookie wall (contains a short message stating that cookies are collected, and an "accept" or an "ok" button to click on) to be amongst the most common styles as well. These most common cookie consent request styles were used to create mock-ups for the current study's user tests, and examples of these designs can be seen in figures 2, 3, and 4 in subsection 5.2.2.

2.1.4 Previous research on users' perceptions of cookie consent requests

As the legislative changes have made cookie consent requests common on websites, they can now be considered ubiquitous. Mejtoft et al. (2021) have found that due to the cookie consent requests' ubiquity users have started to automatically give their consent without properly reading the request's content - also known as a cookie blindness phenomenon. Mejtoft et al. (2023) in their later study found that users care about and are interested in cookies and their privacy, but they still do not read the information on the request well enough to give their informed consent. Similarly, Ha et al. (2006) have found users to perceive that they are not able to make an informed consent. A study by Utz et al. (2019) shows that users often are unsatisfied with cookie consent requests' design and content, and even insecure about their possible effects, sometimes resulting in ignoring the request. Another reason users might be ignoring the cookie consent requests is that due to their frequency and often difficult-to-use or non-user-friendly design, the users are experiencing annoyance, frustration and even consent fatigue when encountering one (Ha et al., 2006; Habib et al., 2019; Kulyk, Hilt, Gerber, & Volkamer, 2018; Mejtoft et al., 2023; Nouwens et al., 2020). Along the same lines, Mejtoft et al. (2023), Ha et al. (2006), and Nouwens et al. (2020) have found that users often see the request as an irritating friction or a distraction in their interaction with the website. Users in the study by Ha et al. (2006) even described cookie consent requests as overly intrusive.

A study by Singh et al. (2022) reveals that users often perceive the cookie consent requests' design as time-consuming and having excess information, as well as having a lack of transparency and customizability. Moreover, Habib et al. (2019) have found users to perceive the cookie consent requests as difficult to use or understand, making it difficult to make a consent choice. They suggest that this could be caused by, among others, a lack of unified terminology and a complex consent-giving process (Habib et al., 2019). Due to this, some users even describe cookie consent request as confusing (Ha et al., 2006; Habib et al., 2019), which might lead the users to make privacy-unfriendly choices (Kulyk, Hilt, Gerber, & Volkamer, 2018). Not only are users confused, but Singh et al. (2022) have found that 71% of 98 participants in their study seemed to be suspicious about the websites that used cookie consent requests and believed that tracking was happening even without their consent. Another user perception of cookie consent requests was found by Habib et al. (2019), when some users in their study described cookie consent requests as purposefully burdensome. When it comes to the users' perceived voluntariness, the users in the study by Nouwens et al. (2020) described the requests to force them to give their consent.

Lastly, it has been suggested that users' general unawareness of cookies' purposes and their effects on users can lead to negative perceptions and emotions (Ha et al., 2006). Another reason for negative emotions may be, as suggested by Utz et al. (2019), that users have a negative presumption about cookies, and they overall do not agree with cookie data collection. To summarize the findings from previous research, cookie consent requests are most often perceived and

described as something negative by the users, leading to uninformed and privacy-unfriendly consent decisions.

2.2 Deceptive design and deceptive patterns

Deceptive design is a general concept that involves creating misleading experiences and pushing users toward choices or actions that might not be in their best interest (Brignull et al., 2023). Within this broader framework, *deceptive patterns*, as defined by Brignull et al. (2023) are specific design elements or tactics intentionally crafted to mislead users.

In this section, deceptive design and deceptive patterns are introduced as concepts, and different types of deceptive patterns are listed with practical examples. Additionally, legislation prohibiting deceptive design is introduced, and previous research on users' perceptions of deceptive design are presented.

2.2.1 Deceptive design elements: deceptive patterns

Deceptive patterns, more commonly known as dark patterns, were first introduced in 2010 after the rise of e-commerce websites that were using deceptive design techniques to mislead consumers into buying more, faster and without a genuine need for buying (Brignull et al., 2023). Instead of the word "dark", the current study, similar to Brignull et al. (2023), uses the term "deceptive" to minimize the impact of the negatively associated word "dark" on people's perceptions. In the current study, deceptive design is used as a common, general term, and deceptive patterns refer to the specific style elements.

Deceptive patterns are specific style elements within a user interface aimed to mislead users (Brignull et al., 2023). An example of a deceptive pattern in a cookie consent request is that the user is guided toward accepting all cookies as the most appealing and easy-to-notice option in the request. Previous studies have shown that deceptive patterns in cookie consent requests often nudge users toward a privacy-unfriendly choice, such as consenting to the collection of all cookies (Graßl et al., 2021; Mathur et al., 2021)

A closely related phenomenon to deceptive design is digital nudging. Digital nudges are design choices that guide the user toward a certain, often positive choice, which results in an outcome that the user was looking for (Acquisti et al., 2018). Deceptive design is different to this, since its main purpose is to mislead users into thinking that they are doing something that benefits them, but instead of the user the company behind the deceptive pattern is the one that benefits more from it (Gray et al., 2018). Brignull (2011) exemplifies this by stating that companies might use deceptive patterns to increase their conversion rates, which - as it was found by Graßl et al. (2021) and Mathur et al. (2021) - might turn out to be a privacy-unfriendly outcome for the user.

Today, cookie consent requests' user interface designs are often offered on Consent Management Platforms (CMPs) from where companies can buy and

simply just copy and paste a piece of code to their own website to add a cookie consent request (Singh et al., 2022). CMPs make it easier for companies to outsource their cookie management process (Santos et al., 2021), and the prevalence of a handful of consent request designs has resulted in unwritten design standardization which has made the requests easier for users to understand and recognize (Singh et al., 2022). Contrary to the positive effects of CMPs, Utz et al. (2019) have found that a minimum of 57,4% of the 1000 CMP designs that they studied used deceptive patterns that nudged the user toward a privacy-unfriendly consent choice.

On their website, Brignull et al. (2023) provide a hall of shame of companies that have been recognized to use deceptive patterns. Some of the most noticeable companies on that list with the most deceptive pattern examples are Google, Amazon, Facebook/Meta, Microsoft and Twitter/X. Brignull et al. (2023) also provide a list of legal cases that have to do with the use of deceptive patterns, with one case being a heart rate monitor and a smart watch manufacturer from Finland. Deceptive design is not only used by big corporations, but instead, it is a common sight to see on the cookie consent requests of all sorts of websites. To exemplify the prevalence of deceptive patterns, Mathur et al. (2019) found 1818 instances of deceptive patterns from 1254 websites that they studied. Similarly, Alharbi et al. (2023) found that over 90% of the 243 e-government websites that they studied used deceptive patterns in their cookie consent requests. In the same vein, Krisam et al. (2021) studied 500 German websites' cookie consent requests from which they found that 85% of them nudged users toward a privacy-unfriendly choice. Although companies might benefit from using deceptive design (Brignull, 2011), the use of deceptive design can lead to negative perceptions in users, possibly damaging the organization's reputation and their customer relationships (Mejtoft et al., 2023).

The ethical side of deceptive design is an important part of research discussion as well. Gray, Santos, Bielova, et al. (2021) found that deceptive patterns raise ethical dilemmas in users, and similarly, Gray et al. (2018) found that design practitioners have several ethical concerns related to the topic. Equally, Graßl et al. (2021) state that using deceptive patterns faces both legal and ethical problems.

2.2.2 Types of deceptive patterns

Brignull et al. (2023) have defined 16 different types of deceptive patterns. Multiple previous studies have been conducted to study the prevalence of these different types of deceptive patterns (see, Alharbi et al., 2023; Gray et al., 2018; Habib et al., 2022; Martini and Drews, 2022; Mejtoft et al., 2021; Soe et al., 2020). Of these 16 types, nine were found more commonly than others in those studies: comparison prevention, confirmshaming, forced action, misdirection, nagging, obstruction, preselection, sneak into basket, and visual interference. Table 1 below includes the definitions of these patterns and gives practical examples of how they could be used in a cookie consent request. Picture examples of deceptive patterns can be seen in figures 2, 3 and 4 in subsection 5.2.2 where the mock-ups for the user tests of this study are introduced.

TABLE 1 Deceptive patterns commonly found in cookie consent requests, with examples

Deceptive pattern	Definition	Example in a cookie consent request
Comparison prevention	"The user struggles to compare products because features and prices are combined in a complex manner, or because essential information is hard to find." ^a	There is no clear option to view details of each cookie category, making it difficult to compare each of their impacts on the users' privacy.
Confirm-shaming	"The user is emotionally manipulated into doing something that they would not otherwise have done." ^a	Decline button says: "No thank you, I want a bad user experience".
Forced action	"The user wants to do something, but they are required to do something else undesirable in return." ^a	The user is required to accept all cookies before getting access to the website, without an option to decline consent.
Misdirection	"The design purposefully focuses your attention on one thing in order to distract your attention from another." ^b	"Accept all" is a big, bright green button, while "decline all" is a very small button and has a light gray color.
Nagging	"The user tries to do something, but they are persistently interrupted by requests to do something else that may not be in their best interests." ^a	The user is repeatedly prompted to accept all cookies each time they enter a new page on the website, despite previously declining consent.
Obstruction	"The user is faced with barriers or hurdles, making it hard for them to complete their task or access information." ^a	Multiple steps and navigating to hidden menus are required to decline cookies. Accepting to all is a simple option.
Preselection	"The user is presented with a default option that has already been selected for them, in order to influence their decision-making." ^a	All cookie categories are preselected by default, encouraging the user to accept to all of them without making their own conscious decision.
Sneak into basket	"The use of reading order manipulation to "sneak" information past the user." ^c	Non-essential and essential cookies are included in the default selection, making it easy for users to overlook and unintentionally accept both.
Visual interference	"The user expects to see information presented in a clear and predictable way on the page, but it is hidden, obscured or disguised." ^a	"Decline all" option is in small, low contrast text that does not look like a clickable button. "Accept all" is the opposite, very easy to notice.

Note:

^aBrignull et al. (2023, Section titled "Types of Deceptive Pattern").

^bGray et al. (2018, p. 4)

^cGray, Santos, Bielova, et al. (2021, Section 4.2.2)

2.2.3 Legislation prohibiting deceptive design

There are multiple legislations in the European Union attempting to ensure fairer design practices on the internet (Brignull et al., 2023). In addition to the GDPR (Regulation 2016/679) mentioned earlier, Unfair Commercial Practices Directive (UCPD; Directive 2005/29/EC) and Digital Markets Act (DMA; Regulation (EU) 2022/1925) apply to the use of deceptive design in some ways. The UCPD (Directive 2005/29/EC) and the DMA (Regulation 2022/1925) prohibit unfair, misleading, and aggressive commercial practices, which could apply to guiding the user toward accepting to all or for example, marketing cookies, which the consumer would not have originally wanted to do.

Additionally, according to the DMA (Regulation 2022/1925), companies are required to share important information that consumers need to make well-informed decisions, which deceptive patterns often disguises. Furthermore, the UCPD (Directive 2005/29/EC) prohibits companies from hiding or obscuring information in any way that could mislead customers. According to the GDPR (Regulation 2016/679) rules that apply to deceptive design, hiding information needed for user's informed consent is prohibited, consent has to be given voluntarily, transparency from data collectors is insisted, privacy as the default option is required, and vague language or preselected cookie choices are not accepted. None of these regulations explicitly ban the use of deceptive design, although they strongly suggest against it.

2.2.4 Previous research on users' perceptions of deceptive design

Much of the existing literature on deceptive design has shown that it raises negative perceptions and emotions in users. In Maier and Harr's (2020) study, users described deceptive patterns negatively as sneaky, hidden, triggering, forcing, and dishonest, viewing the patterns as unethical and manipulative behavior by the organization. The participants were also concerned of the deceptive patterns causing them personal harm (Maier & Harr, 2020). In a study by Bongard-Blanchy et al. (2021), users described deceptive patterns as ridiculous. In the same negative vein, Gray, Chen, Chivukula, and Qu (2021) have as well found that users describe deceptive patterns as aggressive, unprofessional, twisted, misleading, complicated, and difficult. In a study by Lupiáñez-Villanueva et al. (2022), negative perceptions related to deceptive patterns were also prominent. The participants of their study described interfaces with deceptive design to be more difficult to understand, less transparent, and unclear regarding how to complete the action that the user intended.

Maier and Harr (2020) found the users to express negative emotions related to deceptive patterns. The users brought up emotions such as annoyance, anger, irritation, frustration, worry and stress, and feeling stupid or pressured. A similar finding was made by Bongard-Blanchy et al. (2021) who found that deceptive design made the users feel frustrated and anxious. Lupiáñez-Villanueva et al. (2022), as well, made similar findings in their study, reporting that users were feeling stressed, anxious, and annoyed by deceptive design. Similarly, Gray,

Chen, Chivukula, and Qu (2021) concluded negative emotions from their study – the users mainly reported feeling distressed, upset, hostile, and irritable, as well as some of the following emotions: being nervous, afraid, scared, or jittery. Along the same lines, a study by Mathur et al. (2021) concludes that users express more negative emotions after interacting with deceptive patterns.

Some participants in the study by Gray, Chen, Chivukula, and Qu (2021) described that a data collector that uses deceptive patterns is only thinking of their own benefit. Therefore, many participants in their study expressed feeling undervalued as a person when deceptive patterns were used. As another perception, Mejtoft et al. (2023) pointed out that the use of deceptive patterns can make the users suspicious of the website and the organization's trustworthiness and credibility. Quite similarly, some participants in the study by Gray, Chen, Chivukula, and Qu (2021) described that deceptive design makes it feel like something is off or not correct on the website. Furthermore, a study by Lupiáñez-Villanueva et al. (2022) showed that users' trust in an organization was diminished due to deceptive design. Taking the perceptions further, Machuletz and Böhme (2020) found that users often regretted their consent decision after they had consented to the cookie data collection, if they were afterwards informed about the cookies' effect on the users' privacy.

Unlike others, one participant in Maier and Harr's (2020) research mentioned there to be a positive side to deceptive patterns: being pressured helps to make a decision faster. Likewise, contrary to the previously mentioned studies, Keleher et al. (2022) found that the majority of the users in their study generally found deceptive patterns to be more positive (e.g., honest and ethical) than negative, which they assume proves that experts often incorrectly assume users' responses and perceptions. But even in their research, users described deceptive patterns as intrusive, which is a negatively associated description (Keleher et al., 2022).

Contrary to most previous studies, Gray, Chen, Chivukula, and Qu (2021) found that some participants felt sympathy toward an organization that uses deceptive patterns because the participants thought that maybe the organization does not use the patterns on purpose. Additionally, the participants in their study wanted to understand the organization's need to survive financially, which deceptive patterns, as stated by Brignull (2011), help with by increasing the company's conversion rates. Still, some participants in the study by Gray, Chen, Chivukula, and Qu (2021) also described the use of deceptive patterns as short-sighted.

Interestingly, some participants in Maier and Harr's (2020) study seemed to have a resigned attitude to deceptive patterns due to being used to seeing them so much. A similar finding was made by Di Geronimo et al. (2020) who suggested that due to the ubiquity of deceptive patterns, users see it as a part of their normal interaction with websites. Lupiáñez-Villanueva et al. (2022) have similarly stated that users might not see the negative side of deceptive patterns due to their ubiquity.

Previous research has additionally focused on users' knowledge and education on the topic of deceptive design. For example, Di Geronimo et al. (2020) and Keleher et al. (2022) have found that users are not able to recognize deceptive design in the first place. Di Geronimo et al. (2020) suggest that educating users on deceptive design would be the first step in making the users act more careful when it comes to their privacy. As an interesting point, Keleher et al. (2022) have stated that the users could have different perceptions of deceptive design if they were educated on the topic - if they were educated, they would for example, know deceptive design's potential risks. Lupiáñez-Villanueva et al. (2022) made a similar notice - they suggested that users' limited awareness of the topic might cause them to not acknowledge their negative experiences related to deceptive patterns.

Additionally, it should be noted that not only does deceptive design influence users' perceptions, but it also influences users' behavior. The existing literature on deceptive design's impact on users' consent choices is extensive, in contrast to users' perceptions on it. Studies by Machuletz and Böhme (2020) and Nouwens et al. (2020) showed that deceptive design guides the user toward accepting more cookie data collection purposes than they would have initially wanted to. Several studies, such as Habib et al. (2019) and Utz et al. (2019) demonstrated that deceptive design makes it more difficult to decline cookie data collection. Like many other scholars, Mathur et al. (2021) have reported that deceptive design undermines users' privacy by guiding them toward privacy-unfriendly consent choices. Similarly, Mathur et al. (2019) have argued that deceptive design prevents users from being fully informed about cookies and the effects of different consent choices, often leading them to act contrary to their initial intentions. In the current study, the focus is on users' perceptions, not their behavior, and therefore deceptive design's influence on users' consent choice is not more thoroughly investigated.

Lastly, it is important to mention that users' perceptions are always context- or design-dependent, and different deceptive patterns might be perceived with a different level of negativity or positivity (Lupiáñez-Villanueva et al., 2022).

3 PRIVACY AND DESIGN

In this chapter, the concept of privacy and its historical development is introduced from the historical context to the current digital era, concluding with what online privacy implies today. In the latter part of the chapter, privacy-protective design guidelines and attributes are presented, because they provide important insights for interpreting the results and understanding design's influence on users' perceptions of privacy.

3.1 Introduction to privacy concepts and definitions

In this section, the evolution of the definition of privacy is introduced. Key foundational theories of privacy are presented, supported by traditional scholarly perspectives. More importantly regarding the study's context, it is introduced how users define private information. This section establishes the theoretical basis for the complex and always evolving concept of privacy.

3.1.1 Evolution of privacy: historical context

Researchers from multiple fields have tried to conceptualize *privacy*, including psychology (Altman, 1975), law and economics (Posner, 1981; Warren & Brandeis, 1890), political science (Westin, 1967), and information systems (e.g., Culnan & Armstrong, 1999; Smith et al., 1996). There are some similarities between the definitions, but still, there is not only one way to define privacy. Since no common ground has been established in the previous, historical, conceptualizations, researchers have later tried to come up with a common concept of privacy (see e.g., Margulis, 2011; and Smith et al., 2011).

The first definition of privacy dates back to the late 1800's when Warren and Brandeis (1890) argued for the recognition of a person's legal right to privacy, stating that individuals have the right "to be left alone and able to control the release of his or hers personal information". The conceptual development of privacy has been divided into four stages by Westin (2003), and these stages are

followed in this subsection when introducing the historical development of privacy. To start with, the baseline for privacy was created after the second World War (1945-1960) when the development of information technology was on the rise, although not much importance was put on the privacy perspective (Westin, 2003).

The second stage of privacy development happened around 1961-1979 when central data bank projects and third-generation computer systems with remote access were developed (Westin, 2003). During this period, Westin (1967) and Altman (1975) coined their primary theories of privacy, defining privacy as one's personal control over information sharing. Westin (1967) identified four states of privacy: solitude, intimacy, anonymity and reserve. Additionally, he defined four purposes of privacy: personal autonomy, emotional release, self-evaluation, and protected communication (Westin, 1967). Altman (1975) expanded Westin's definition, defining privacy as "the selective control of access to the self" (p. 24). Altman's (1975) definition focuses on the fluid nature of privacy and introduces the idea of four zones: intimate, personal, social, and public - within which the expectations of privacy vary based on cultural influences. Altman's (1975) preliminary idea of privacy as a social, psychological, and cultural process was later supported by Waldo et al. (2010) who stated that privacy is context-dependent and prone to changes. In 1977, Margulis made an attempt to unify Westin's (1967) and Altman's (1975) theories by concluding that privacy "represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance the autonomy and/or to minimize vulnerability" (Margulis, 1977, p. 10).

The third stage of privacy development happened between 1980-1989, during which the importance of privacy did not increase or change, but on the other hand, the first privacy protection acts were enacted due to enhanced computer performance (Westin, 2003). During this time, Posner (1981) created a new definition of privacy emphasizing the importance of an individual's ability to control and protect their personal information and decisions, and seeing privacy from three perspectives: secrecy, seclusion, and autonomy. Privacy as secrecy views privacy as an individual's ability to control and limit access to their private information (Posner, 1981), similar to Westin's (1967) concept of reserve. Privacy as seclusion refers to the physical and psychological space away from others (Posner, 1981), similar to Westin's (1967) solitude state. Finally, Posner's (1981) definition of privacy as autonomy refers to an individual's right to be in charge of their own decisions and information without others' interference, with personal freedom and self-determination as main concepts. Autonomy is a unique dimension in Posner's (1981) framework, when compared with the one by Westin.

The fourth stage of privacy development happened during the turn of the millennium (1990-2002), characterized by the rise of the Internet and modern technologies such as mobile phones (Westin, 2003). This is when privacy started to become a prioritized issue both socially and politically (Westin, 2003). In 1999, Pedersen supported Westin's (1967) four states of privacy (solitude, intimacy, anonymity, and reserve) and uniquely extended them with creativity, highlighting

that not only should individuals be protected from others but also be able to freely engage in creative activities and explore ideas without external pressure (Pedersen, 1999).

To conclude, Posner's (1981), Pedersen's (1999), and Westin's (1967) perspectives – solitude, intimacy, anonymity, autonomy, and creativity - combined provide a comprehensive basis for privacy. On top of those, the changing nature and complexity of privacy, as well as individuals' constantly changing needs influence the concept's definition (Westin, 2003). Moving forwards, technological change has brought new dimensions to the concept of privacy, which will be discussed next.

3.1.2 Evolution of privacy: the digital era

Modern technologies and the commercialization of the Internet have required the concept of privacy to change and adapt (Westin, 2003). Waldo et al. (2010) have identified three drivers of change for privacy: technological change, societal shifts, and discontinuities in circumstances (e.g., sudden changes in people's privacy concerns due to data breaches). These drivers have made privacy in the digital era more complex than ever, as individuals are now facing new privacy concerns in online environments (e.g., Malhotra et al., 2004).

As the concept of privacy has adapted to the digital era, its definition has shifted from a traditional concept of personal rights and limits to one's information, to a complex process of data management and control over privacy. Alharbi et al. (2023, p. 2) define internet privacy as "the ability to control the personal information users want to share on the internet", highlighting that individual's control over their data has become a central part of understanding modern privacy.

Online data collection, according to Chellappa and Sin (2005), involves various types of information of individuals, such as anonymous, personally unidentifiable, and personally identifiable information. However, not all this data might necessarily be considered private by the person, as each individual, according to Petronio (2016), defines private information differently. Petronio (2016) suggests that an individual's information is considered private, as soon as the person starts thinking of any of the following questions: Who knows about this information? Who is restricted to this information? How much do others know about this information? When is this information told to someone? And when is this information concealed from others? Another way to tell if the person finds the information private is when the individual shows behavioral indicators of wanting to manage their private information (Petronio, 2016). These considerations are important in the interviews of the current study, when participants define the level of privacy that they perceive to have or the personal importance of information privacy for them.

As online data collection has increased, so have individuals' online privacy concerns (Antón et al., 2010). As a result, multiple privacy concern scales have been developed, of which, the scale for Internet Users' Information Privacy Concerns (IUIPC) by Malhotra et al. (2004) is commonly used. The IUIPC scale

emphasizes individuals' concerns around the collection of their private data, their personal control over privacy, and their awareness of information privacy practices. This increase in privacy concerns has also made individuals more aware and interested in the following questions regarding their privacy: 1) what type of personal data is collected; 2) who the data is shared with; and 3) if the data is sold to third parties (Barth et al., 2022).

Growing concerns have had a regulatory impact as well. The rise of data collection technologies, such as cookies, has pushed policymakers to regulate online data collection more precisely, carrying out legislations such as the GDPR (Regulation 2016/679) and the ePrivacy Directive (2002/58/EC), as introduced in section 2.1.2 Cookie compliance. Additionally, other tools and ways of protecting privacy have emerged due to the increased concerns and risks that an online environment opposes to privacy. As a broad example, Waldo et al. (2010) present eight tools of protecting privacy: personal unilateral actions (self-help), technology, policy, limits on outsider access, prevention of internal abuse, notification, correction, and Fair Information Practices. Individuals, organizations, and governments should all take action in these areas to enhance privacy (Waldo et al., 2010).

Despite the many changes in the definition of privacy and the many challenges that it faces in the modern day, privacy still remains important to both individuals and organizations. As technology keeps evolving, so does the need to adapt the understanding and definition of privacy, making it a dynamic and highly context-specific concept.

In this study, privacy is seen as the protection of an individual and their property. It includes three main points of views, drawing from previous research: a) an individual should have the right and consent over their own information, b) the individual's information should be concealed from third parties, and c) the solitude of the individual should be preserved. On top of the traditional definitions, Westin's (2003, p. 451) conclusion of privacy as a "quality of life topic" is a good way to conclude the importance of privacy on a personal level.

3.2 Privacy-protective design

Since the protection of users' personal information has gotten more important as technology develops and pushes the concept of privacy to change, it is also increasingly important to think of how privacy can be better protected in the digital era. One of the measures to protect users' privacy is through design, and this section introduces two different privacy-protective design frameworks that have been established.

The first one of the privacy-protective design frameworks used as a guideline in this study are *Privacy by Design* (PbD) principles introduced by Cavoukian in 2010. According to her, the PbD principles could mitigate users' privacy concerns and improve the protection of personal data. She proposed seven foundational principles for creating useful and usable privacy interfaces, such as cookie

consent requests. She also notes, that adhering to the Fair Information Practices (as introduced in subsection 4.3.2 Control over privacy) can help in improving users' privacy. The following seven PbD principles (Cavoukian, 2010) are intended for designers to use as guidelines at every stage of an interface design process:

- The interface should be proactive, not reactive, and preventative, not remedial.
- Privacy should be the default setting that provides privacy to the user, even if they have not changed the settings themselves yet.
- Privacy should be embedded into the design as a core functionality, and not be a separate function or an additional setting.
- Privacy should offer full functionality, supporting both legitimate privacy interests and any privacy objectives, without requiring compromises or diminishing another component's importance.
- Privacy should provide end-to-end protection for users' private data – their data should be kept private during its whole lifecycle in the organization and deleted appropriately when needed.
- The organization's privacy practices should be visible and transparent.
- Users' privacy should be respected, prioritizing user interests and empowering user-centricity with privacy-defaults, appropriate notices, and user-friendly design choices.

These PbD principles (by Cavoukian, 2010), when applied to cookie consent requests, could counter any deceptive design practices that are privacy-unprotective. To exemplify the importance of these principles for a user's privacy, a cookie consent request designed following these principles could look as follows. First, the request would be proactive, appearing immediately on the page informing the user about the use of cookies before any cookie data collection begins. Then, there would be no preselected cookie categories, as the most privacy-protective default setting is to only have the essential cookies selected. Additionally, the design should prioritize user's control by offering clear and accessible choices. Lastly, the user's data would be protected end-to-end, with transparent information presented to the user about cookies' purpose, use, and storage. (Inspired by the PbD principles by Cavoukian, 2010.)

Since there is a great deal of research on the topic of PbD by now, a systematic literature review on it has been carried out by Barth et al. (2022). Barth et al. (2022) gathered together the current approaches to understanding online privacy, concluding with thirteen *privacy attributes* related to privacy visualizations. Privacy visualizations are design interfaces - such as cookie consent requests - that an organization uses to communicate their privacy measures and legislative compliance to the users (Barth et al., 2022). Cookie consent requests can be considered a privacy visualization because they inform the users about the organization's data collection purposes and methods and make them understandable to users so that they can make an informed consent-decision. The privacy attributes by

Barth et al. (2022) focus on specific characteristics that are essential for protecting users' privacy. In this thesis, it is expected that privacy visualizations could also contribute to a more positive perception of privacy by establishing a foundation of trust between the users and the data collector – and therefore, the use of deceptive design could possibly influence how users perceive some of these attributes in a cookie consent request. The fifteen privacy attributes by Barth et al. (2022, pp. 20-21) are as follows:

- **Accountability** = “Can the service provider be held accountable for violations?”
- **Anonymization** = “Are all identifiable markers completely removed so that data can never be tracked back to a single person?”
- **Collection** = “Which data are collected?”
- **Control** = “Must the data subject provide consent for collection and processing of their data and to what extent is the data subject able to opt-out of data collection or processing?”
- **Correctness** = “Are there mechanisms for preventing and fixing incorrect data?”
- **Disclosure** = “What is the attitude of the service provider toward requests from law enforcement?”
- **Functionality** = “Is the user forced to choose between functionality and privacy?”
- **Purpose** = “What is the collected data used for?”
- **Pseudonymization** = “Are personally identifiable markers replaced by artificial identifiers, or pseudonyms, such that data can only be traced back to individual users with the help of additional information?”
- **Retention** = “How long is the collected data stored?”
- **Right to be forgotten** = “Can data subjects request that all personal data be removed?”
- **Sale** = “Are any of the data sold to third parties?”
- **Security** = “What technical measures are taken to ensure that data are protected from unauthorized or malicious access?”
- **Sharing** = “Does any of the collected data leave the ownership of the service provider?”
- **Transparency** = “Is the user able to obtain information with regards to how their personal data are handled?”

These privacy attributes by Barth et al. (2022) should be considered when designing privacy visualizations, as they are important regarding how users perceive an organization's privacy measures. By making sure that each of the attributes' questions are answered during the design process and transparently communicated to users in a privacy visualization - such as a cookie consent request - users' privacy perceptions may improve (Barth et al., 2022).

The PbD principles and the privacy attributes were used in this study during the interviews' design theme. The participants were asked questions related

to most of these points, in relation to how they perceive them in a cookie consent request, and how the use of deceptive design might influence their perception of the attribute/principle. In the data analysis, some of these attributes and principles were used as codes, and they were taken into account when pinpointing specific parts of the users' privacy perceptions. Additionally, these privacy protective-design frameworks are referred to when giving suggestions for a more privacy-protective cookie consent request design.

In addition to the above-mentioned privacy-protective design frameworks, multiple researchers, such as Kulyk, Mayer, Käfer, and Volkamer (2018) have attempted to create more simple cookie consent interfaces to assist users in choosing a privacy-friendly setting. Their suggestion of such interface design includes a virtual assistant that guides the user with questions toward their preferred cookie settings, while maintaining an option to adjust the settings manually as well. Additionally, multiple researchers (e.g., Alharbi et al., 2023; Habib et al., 2019; Singh et al., 2022; Kretschmer et al., 2021; Ha et al., 2006) have emphasized the need for privacy-protective design in cookie consent requests, as well as given suggestions on how to achieve that. The suggestions are not further delved into in this thesis, as the focus is not on design suggestions, but rather on users' perceptions.

4 THEORETICAL FRAMEWORK FOR THE PERCEPTION OF PRIVACY

In this chapter, the theoretical framework for the perception of privacy is proposed, consisting of four influencing factors: privacy concerns, control over privacy, trust in the (cookie) data collector, and perceived privacy risks. The framework is inspired by previous models of perceived privacy (by Adams, 1999; Chang et al., 2018; Dinev et al., 2013), which are briefly presented in this chapter as well. Additionally, the role of design in this framework is presented, as guided by the purpose of this study. Lastly, previous research regarding any findings related to users' perceptions of privacy and its four influencing factors in the contexts of cookie consent requests and deceptive design are introduced.

4.1 Overview of the framework

In this study, the theoretical framework for the perception of privacy consists of four influencing factors: users' privacy concerns, control over privacy, trust in the (cookie) data collector, and lastly, their perceived privacy risks. Each of these factors contribute to a user's overall perception of privacy. The goal of this study is to investigate how design, more specifically deceptive design, influences this overall perception and the four influencing factors within, and therefore design is added to the framework as a possibly influencing factor. The context of this study is cookie consent requests, to which the framework is applied to. Figure 1 below illustrates the theoretical framework for the perception of privacy, highlighting design's position in it. This framework, when compared with previous models and frameworks, uniquely takes a comprehensive, user experience-oriented perspective on privacy, and incorporates the design factor in it.

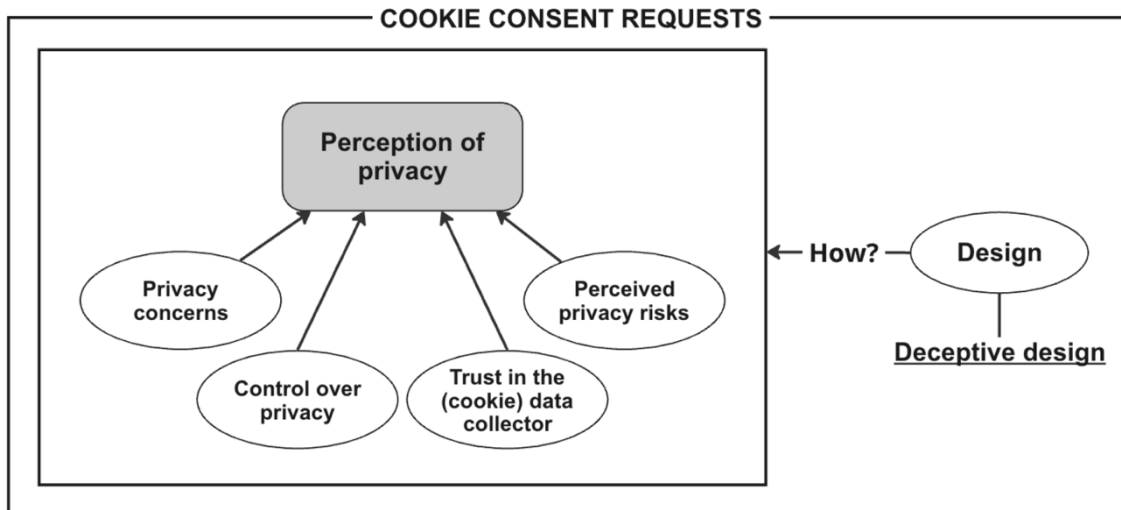


FIGURE 1 The study's theoretical framework for the perception of privacy

While previous studies (Adams, 1999; Chang et al., 2018; Dinev et al., 2013) have studied perceived privacy, the current study attempts to make a difference between *perceived privacy* – a measurable, rational, and often static concept – and the *perception of privacy* – a fluid, subjective user experience. The current study's framework differs from the previous models of perceived privacy by taking a more flexible, and user experience-oriented perspective to the topic in order to capture users' comprehensive impressions and perceptions of the topic at hand, from a privacy-perspective.

Previous research has not yet defined the meaning of perception of privacy, but in this study, it is suggested that it entails users' broader understanding, feelings, impressions, responses, and beliefs of the state of their privacy, making it suitable for qualitative studies where users' can more flexibly express their thoughts compared to quantitative methods. For example, the outcome for a perception of privacy could be that the user perceives the state of their privacy as protected, respected, compromised, undervalued, or unimpacted. It is expected that these perceptions would stem both from the four influencing factors introduced in the current study's framework, as well as other impressions that the users might have. The core question behind the perception of privacy in this study is: "How well does the user perceive their personal information being kept confidential and under their own control?", based on the definition given for privacy in chapter 3.

The definition and content for this study's framework for perception of privacy derived from previous models for perceived privacy (Adams, 1999; Chang et al., 2018; Dinev et al., 2013). The models were examined regarding their suitability for conducting this qualitative study. It is important to note, that the current study's framework is experimental and not used in previous research in its current shape.

Compared with the definition of perception of privacy, perceived privacy could be used to define a certain amount or level of privacy in a specific context, and thus suits quantitative studies better, such as the models by Dinev et al. (2013)

and Chang et al. (2018) have shown. Dinev et al. (2013, p. 299) conceptualize perceived privacy as “an individual’s self-assessed state in which external agents have limited access to information about him or her”.

It is important to acknowledge that multiple other factors can also influence how users perceive their privacy. These include the participants’ demographics such as their gender, age, education, and income (as introduced in Chang et al., 2018), their personal characteristics like personality traits and previous experiences (see e.g., Bansal et al., 2010), and their knowledge of privacy practices (e.g., Ha et al., 2006; Keleher et al., 2022). Additionally, information sensitivity (Chang et al., 2015), and cognitive load (Nouwens et al., 2020) have been found to influence privacy perceptions. Lastly, brand reputation can also have an influence (Brakus et al., 2009). However, due to the scope of this study and resource limitations, it is not possible or of interest to study the influence of all these factors, and thus, the framework only focuses on the four main influencing factors, as included in the models by Adams (1999), Chang et al. (2018), and Dinev et al. (2013).

The theoretical framework is used in the preparation of the interview themes and questions. Additionally, it is used as a theoretical lens for analyzing data to conclude an overall finding of the perceptions of privacy and understand the influence of deceptive design on this perception. Next, the three previous models for perceived privacy (by Adams, 1999; Chang et al., 2018; Dinev et al., 2013) are presented, as they have inspired the configuration of this framework.

4.2 Previous models inspiring this framework

Three models on perceived privacy by Adams (1999), Chang et al. (2018), and Dinev et al. (2013) were used as a basis and inspiration for the theoretical framework used in this study. Here, it should be paid attention to the distinction between perceived privacy and perception of privacy, as introduced in the previous section. Despite previous models focusing on users’ perceptions on the four influencing factors individually, no prior model has looked at how all these four factors contribute to the overall user experience-oriented perception of privacy, and what kind of role (deceptive) design has in shaping the perception.

The first of the three main models for perceived privacy was coined by Adams in 1999. Adams’ model attempts to explain perceived privacy and its effect on users’ attitudes and behavior in multimedia communication environments. The model consists of three main factors for the user’s perceived privacy: information sensitivity, information usage, and information receiver (Adams, 1999). First in the model, the user judges the level of their personal information’s sensitivity. Second, the user evaluates whether they trust the information receiver (also known as data collector), and whether the information shared with them is too vulnerable not to share. Third in the model, the user balances the perceived risks and benefits of sharing information with the data collector, influencing the user’s willingness to share data with them. Regarding the risk-benefit

balance, the user considers how the information is used by the data collector (Adams, 1999). All these three factors affect each other in one way or another, finally creating the idea of perceived privacy in Adams' model. From this model, user's trust in the data collector and the user's consideration of the risk-benefit balance was taken to the current study's theoretical framework, as they were also included as main influencing factors in the models by Dinev et al. (2013) and Chang et al. (2018). Additionally, the information sensitivity aspect from Adams' (1999) model was used in this study during the interviews when trying to understand users' disposition to their privacy and their perceived sensitivity of cookie data, as a foundation and context to discussing the users' perceptions of privacy more in depth. Despite Adams' (1999) model having usable ideas for the current study's framework, the model as a whole was considered too narrow to directly use in the current study for understanding users' comprehensive perceptions of privacy, as modern technologies and online environments have already proposed other factors that influence users' perceived privacy after the introduction of the model in 1999. These additional factors can be seen in the models by Chang et al. (2018) and Dinev et al. (2013) that are introduced next.

The second of the three models for perceived privacy was coined by Chang et al., first in 2015, later expanding and modifying their model in 2018. The 2018 version of their model was used as inspiration for the current study's theoretical framework. The model of Chang et al. (2018) for perceived privacy is called the Privacy Boundary Management model, in which the end state is perceived privacy. The focus of the model (Chang et al., 2018) is on understanding how individuals evaluate the adequacy of institutional-level privacy policies and practices. The model explores whether a user perceives that their personal information will be secured and managed well by the data collector, balancing this perception with the user's need for their personal information to be handled with trust and assurance that their data will remain private. The model (Chang et al., 2018) explores how individuals ultimately come to a decision of their privacy boundaries - deciding what information they want to keep to themselves and what information they want to share with others - after assessing the confidentiality of their private information and the perceived security of the privacy policies and practices. In this model, the final decision of the individual's privacy boundaries is their perceived privacy. Chang et al. (2018) have defined that a user's idea of their control, existing risks, possible concerns, and trust in the service or data collector all have an influence on the user's perceived privacy. These four influencing factors are similar to the current study's theoretical framework, but the difference is that Chang et al. (2018) use these factors as measurable constructs that lead to the ultimate decision of the individual's willingness to share their private information with the data collector, unlike the current study's framework which defines perception of privacy as a subjective user experience that includes the individual's thoughts, understanding, feelings, impressions, responses, and beliefs of the ultimate state of their privacy. The model by Chang and colleagues is very similar to the current study's framework, but the difference is mainly in the way that they are used: by measuring the privacy (the study by Chang et al., 2018)

versus exploring and examining the privacy (the current study's framework). Additionally, different to the model by Chang et al. (2018), the current study looks at the individual influencing factors from a broader perspective than just a positive-negative scale, including the individual's comprehensive impressions, attitudes, and experiences related to the factors within the study's context (see section 4.3).

Similar to the current study's framework, Chang et al. (2018) consider perceived trust and control to enhance the perceived privacy, and perceived privacy risks and concerns to diminish the perceived privacy. Chang et al. (2018) have statistically proven that these factors influence the individual's perceived privacy. In their model, Chang et al. (2018) have also included the Fair Information Practices (FIPs; Federal Trade Commission, 1998) as antecedent factors of boundary-identification. They state that FIPs are important factors to consider in further studies, since their effect on boundary-identification is remarkable. Therefore, FIPs were used as guiding questions in the interviews of the current study, and they are more closely presented in subsection 4.3.2 Control over privacy.

The third model of perceived privacy was created by Dinev et al. in 2009, and further developed and improved in 2013. The 2013 model by Dinev et al. is used as inspiration in the current study's theoretical framework. In their model, perceived privacy is considered an individual's privacy attitude, which is based on their perceived control over their privacy and the perceived privacy risks (Dinev et al., 2013). These two factors are included in the current study's theoretical framework as well. In their previous model, Dinev et al. (2009) included an aspect of vulnerability of their private information, similar to the model by Adams (1999). This vulnerability-aspect included privacy concerns (Dinev et al., 2013), that also Chang et al. (2018) has identified as an influencing factor on perceived privacy. Although, the later model by Dinev et al. (2013) left out the concern factor because it was considered more of an outcome rather than an input in the decision-making process regarding privacy, and the researchers decided to instead focus on the underlying factors, like information sensitivity, information transparency, and regulatory expectations. In the current study, privacy concerns factor is included in the framework, as the study specifically looks at the concerns as "outcomes" in the users' overall perceptions of privacy. The earlier model by Dinev et al. (2009) showed that perceived privacy was based on individuals' privacy values and privacy beliefs, but the further developed model (Dinev et al., 2013) left out this idea, and instead focuses on the influence of control and risks to perceived privacy, as with them it is easier to capture variability of privacy perceptions in different contexts. In the current study's framework, values and beliefs are in a central role in understanding users' perceptions, as the framework is only designed for a specific context (cookie consent requests and design). Regarding the perceived control factor, Dinev et al. (2013) introduce three influencing factors for it: anonymity, secrecy, and confidentiality. Anonymity measures how well the individuals perceive to be able to hide their identity; secrecy measures the individual's ability to keep back their information from others; and confidentiality measures how well the individual thinks that their information is

being stored confidentially (Dinev et al., 2013). These anonymity and secrecy factors were taken into account in the data analysis part of this study when attempting to understand the participants' perceptions of control over their privacy. Lastly, an additional significantly influencing factor for perceived privacy in Dinev and colleagues' model (2013) is how users balance the perceived risks with the expected benefits of sharing their data or using the service - this idea is included as an important determinant of users' perceived privacy risks in the current study's framework. This risk-benefit evaluation (known as privacy calculus theory) is more closely introduced in subsection 4.3.4 Perceived privacy risks.

The model for perceived privacy by Dinev et al. (2013) was neither a fully comprehensive model for examining users' overall perceptions of privacy, as some key factors such as concerns and trust (both introduced by Chang et al., 2018; trust introduced by Adams, 1999) were missing from it. Therefore, the current study's theoretical framework includes parts from each of the three above-presented models of perceived privacy to gather as comprehensive perceptions as possible. Similar to the model by Chang et al. (2018), the model of Dinev et al. (2013) attempts to mainly understand the reasoning behind users' behavior - for example, regarding the decision to share private information with someone - which is contrary to the current study's goal of understanding users' overall, comprehensive perceptions and impressions. Furthermore, the models of Chang et al. (2018) and Dinev et al. (2013) both have a predictive focus, as they are designed to be used in a quantitative, statistically measurable research. In the current study, it is not attempted to predict users' perceptions or use a hypothesis, although the influencing factors picked from the three previous models are used as guiding themes throughout the study - making a distinction between using the factors as guiding themes rather than measurable variables.

To summarize, the influencing factors repeated in each of the three previous models (by Adams, 1999; Chang et al., 2018; Dinev et al., 2013) were used as guiding themes in the current study's theoretical framework. This framework, compared to the three previous models, attempts to take a qualitative, flexible and user experience-oriented perspective on the topic to comprehensively capture users' overall perceptions of privacy. As design's influence is not considered in the previous models, this study uniquely includes it in the framework. Next, the four main influencing factors - guiding themes - included in the current study's framework are more closely introduced.

4.3 Influencing factors within the framework

In this section, the four main influencing factors for users' perceptions of privacy are introduced more in depth. Each subsection first explains the concept and introduces how it has been found to connect to privacy perceptions in previous models and studies. Additionally, any applicable theories or models for measuring or explaining the factors are introduced, as they will be used in the interviews as guiding questions for an in-depth understanding of users' perceptions of the

factor. Likewise, the theories and models related to the factors are used in interpreting the results regarding each influencing factor. An overview of this study's interviews and guiding questions can be found in appendix 1.

4.3.1 Privacy concerns

The first of the five influencing factors used in this study as guiding themes is privacy concerns. Privacy concerns, according to Smith et al. (1996) and Malhotra et al. (2004) are users' concerns regarding the collection, control, storage, use, and sharing of personal information. Privacy concerns' influence on individuals' privacy perceptions has previously been proven by Chang et al. (2018), among others. Additionally, Smith et al. (2011) have found that privacy concerns have an influence on perceived privacy risks and users' perceived trust (Smith et al., 2011). Due to these supporting findings, the privacy concerns factor was added to the framework.

Westin (as cited in Kumaraguru & Cranor, 2005) created an index for understanding individuals' general privacy concerns in 1990. His privacy concern index consists of four questions about concerns regarding: threats to the individuals' personal privacy, organizations collecting excessive personal information about them, the government invading their privacy, and lastly, their control over their personal privacy.

Another way to measure and understand users' privacy concerns is the Concern for Information Privacy (CFIP) scale by Smith et al. (1996). The CFIP-scale divides privacy concerns as related to the collection of personal data, unauthorized secondary use of personal data, improper access to personal data, and errors (Smith et al., 1996). The CFIP scale was created during the early development of Internet and focused on traditional, offline marketing. A more modern version of this scale was created after the commercialization of Internet. This model is called the Internet Users' Information Privacy Concerns (IUIPC) scale by Malhotra et al. (2004). The IUIPC-scale covers three main concerns: collection, control, and awareness of information privacy practices. The IUIPC scale more precisely covers the individuals' awareness of the use of their individual data (Malhotra et al., 2004). With the earlier CFIP-scale (Smith et al., 1996) people were mostly concerned about the errors in their data since the data-handling was mainly done by individual organizations. Whereas the later IUIPC-scale by Malhotra et al. (2004) showed people to be less concerned about the errors since they could now control that themselves. The development of the IUIPC-scale showed people's concerns to revolve around their awareness of the use of their personal data since the digital era has increased the amount of data and possibilities to use it (Malhotra et al., 2004).

In this study, Westin's privacy concern index in addition to the CFIP- and IUIPC-scales were used in creating the guiding questions for the interview theme of privacy concerns to better understand what kind of concerns users have of cookie consent requests that include deceptive patterns.

Lastly, Xu et al. (2011) have defined that privacy concerns are affected by the user's perceived control of privacy and privacy risks, which in turn are

affected by individual's perceptions of the organization's privacy practices and coherence to them. Therefore, the privacy concerns theme in this study's interviews included this idea by Xu et al. as a guiding question for better understanding users' privacy concerns. Additionally, Xu et al. (2011) stated that an individual's disposition to value their own privacy is an important influencing factor when it comes to their privacy concerns. Likewise, the participants in the current study were asked what their general disposition to value privacy is, to better understand their concerns and their extent.

To conclude, there are a multitude of ways to be concerned about one's privacy, and as previous research (such as, Chang et al., 2018) has shown, privacy concerns may have an influence on users' privacy perceptions. Therefore, the previous scales and frameworks mentioned in this subsection for understanding individuals' privacy concerns were used as guiding interview questions in this study within the privacy concerns theme.

4.3.2 Control over privacy

Control as defined by Xu et al. (2011) is the user's perception or belief of their ability to manage the release and distribution of their personal information. Control, in this study, refers to the user's perception of how much control they perceive to have over giving their cookie consent choice. The control over privacy factor was added to the framework, as it has been previously proven to influence individuals' perceived privacy (e.g., Chang et al., 2018; Dinev et al., 2013). Chang et al. (2018) in fact found control to have the biggest influence on perceived privacy, which is why this factor is especially important to include in this study's theoretical framework. Additionally, control was already mentioned in the earliest privacy definition by Warren and Brandeis (1890) who defined privacy as the individual's ability to control the release of their personal information. Taking it further, Chang et al. (2018) have proven control to affect an individual's trust in the data collector, and Acquisti et al. (2015) have found that perceived control reduces the individual's privacy concerns. So, the connection of control to the whole framework of perception of privacy is diverse.

In addition to the previous theories of perceived privacy, control also appears as a factor in relation to users' privacy concerns (e.g., Malhotra et al., 2004; Xu et al., 2011). For example, in the IUIPC-scale the concept of control was related to the individual having "freedom to voice an opinion or exit" the consent-giving situation (Malhotra et al., 2004, p. 338). And in the study by Chang et al. (2015) control measures the power given by organizations for the individual to manage the sharing and collection of their private data.

Possibly the most recognized theory related to the control of one's privacy is Petronio's (2013) Communication Privacy Management model (CPM), that focuses on how an individual manages their privacy boundaries. In this study, the 2013 version of Petronio's CPM model is used, although the model dates back to its original development in 1991 and further refinement in 2002. The CPM model involves an idea of the individual creating a border between their private and public information, based on a set of rules and criteria that they find important

(Petronio, 2013). The model has later been used as a basis for other theories and methods related to privacy (e.g., Chang et al., 2018; Xu et al., 2011). Chang et al. (2018) have statistically proved the effect of boundary identification to boundary rule-formation and ultimately to perceived privacy. This idea of boundary management and boundary formation was used in this study's interviews as guiding questions to better understand how users want to be able to control their privacy, as well as how well they perceive to be able to do it.

Besides the CPM model, Dinev et al. (2013) introduced three concepts related to users' perceived privacy: anonymity, secrecy, and confidentiality. Of these, anonymity measures how well the individual perceives to be able to control their identity, and secrecy measures the individual's ability to keep back their information from others. These two factors were considered when forming an understanding of the users' perceived control in this study's data analysis.

Most importantly, the FIPs, as introduced by The United States' Federal Trade Commission in 1998, were used as guiding questions in this study's interviews to understand participants' perceptions of control. Chang et al. (2018), in their privacy boundary management model, mention FIPs as important influencing factors to the individuals' perceived privacy, especially regarding the control of their privacy boundaries. FIPs are defined into four distinct principles for ethical and responsible collection of individuals' personal information: notice, choice, access, security, and in later versions of FIPs (Federal Trade Commission, 2000) even enforcement. Notice as a FIP principle refers to individuals being informed about how their data is being collected, handled and shared (Federal Trade Commission, 1998). Choice as a FIP principle refers to the individuals' choice to opt-out or control the use and collection of their personal information (Federal Trade Commission, 1998). Access as a FIP principle considers the individual's right to access their personal information collected by organizations and to be able to verify, review, and delete it (Federal Trade Commission, 1998). Security as a FIP principle refers to the technical safeguards that the data collector should use to ensure that there is no unauthorized access or disclosure of private information (Federal Trade Commission, 1998). Enforcement as a later introduced FIP principle, refers to the data collectors' adherence to the legislative acts of privacy, with the possibility of taking legal action in case of any regulative infringement (Federal Trade Commission, 2000). Similar to Chang et al. (2018), the FIPs were used in the interviews of the current study as a helpful set of concepts to understand the big picture of how the participant perceives the data collector to adhere to ethical and responsible data collection - also highly relating to the next introduced influencing factor: trust in the cookie data collector - and how well the data collector is perceived to provide control for the user.

To conclude, there are multiple previous theories and models pointing out control's importance for users' privacy, which makes it an important factor to include in this framework. Various theories and principles were utilized in the interviews of this study to understand how well users perceive to be able to control their privacy, regarding their freely given consent to share or not share their cookie data.

4.3.3 Trust in the (cookie) data collector

The influence of trust on perceived privacy has been previously identified in the models of Chang et al. (2018) and Adams (1999), and therefore it has been added to this theoretical framework of perception of privacy as well. There are some other connections related to trust as well within the same framework. Malhotra et al. (2004) have stated that control is an influencing factor to trust, and Pavlou (2003) has shown trust to influence perceived risks as well.

Trust has multiple definitions intended for different contexts. In this thesis, the original definition of organizational trust by Mayer et al. (1995) and the definition of web trust by McKnight et al. (2002) are used. Both studies include multiple levels or layers of trust, which are used as guiding questions in the interviews of the current study to help the participants more comprehensively identify their trust in the cookie data collector. Additionally, these previously identified layers and levels of trust helped in interpreting the data related to the users' general trust and all its dimensions together.

Mayer et al. (1995, p. 712) define trust as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”. Mayer et al. (1995) identified the following three key factors for perceived trustworthiness:

1. **Ability** of the trustee: the trustee is able to fulfill their responsibilities for example, regarding using responsible methods for storing data.
2. **Benevolence** of the trustee: the trustee has good intentions behind using the trustor's data.
3. **Integrity** of the trustee: the trustee adheres to the privacy legislation and their own privacy policy.

McKnight et al. (2002) instead take the definition of trust into the digital era, and divides the concept of web trust into the following four constructs:

1. **Disposition to trust:** the trustor's general willingness to trust others.
2. **Institution-based trust:**
 - a. The trustor's belief that the overall web environment, including its legislation and technological functionality, are trustworthy, functional, and secure.
 - b. The trustor's belief that the trustee adheres to these legislations and that their technology functions reliably.
3. **Trusting beliefs:** the trustor's perception of the trustworthiness of the trustee, based on the three attributes of trust defined by Mayer et al. (1995): ability, benevolence, and integrity.
4. **Trusting intentions:** the trustor's willingness to depend on the trustee, for example, by sharing private information with them.

Gefen and Straub (2004) have noted that predictability should be added to the definition of trust in order to create a concept of e-Trust that even better captures the modern trust of a user in a digital space. Predictability refers to the trustor's expectation of the trustee to behave reliably, reducing the trustor's uncertainty about the relationship (Gefen & Straub, 2004).

To conclude, the concept of trust is broad and captures the users' trust comprehensively from multiple perspectives. As trust already has a stable position in some models of perceived privacy, it is added to this framework of privacy perceptions as well. The previous scholars' definitions of trust, as well as the varying perspectives on it are used as guiding questions throughout the interviews.

4.3.4 Perceived privacy risks

Chang et al. (2018) and Dinev et al. (2013) have both proven perceived privacy risks to have a direct influence on perceived privacy, and therefore the factor was also added into this study's framework.

An important theory related to privacy risks is privacy calculus. It helps in understanding users' privacy behavior related to the sharing of their personal data, as the user weighs the potential risks with the expected benefits of sharing information with the data collector (Dinev & Hart, 2006). The theory was first coined in social sciences by Laufer and Wolfe (1977), and later modified to match IT research needs by Culnan and Armstrong (1999). After the commercialization of the Internet, Dinev and Hart (2006) further extended the theory to match the digital behavior of users. In this extended theory, risks were replaced with risk beliefs, consisting of sharing information to third parties and misuse of information (Dinev & Hart, 2006). Benefits were also replaced with confidence and enticement, consisting of: trust in the trustee, reliability of the situation and the trustee, safety of the environment, and personal motivation to sharing information (Dinev and Hart, 2006). In the extended privacy calculus theory, perceived risks also affect the individuals' privacy concerns (Dinev & Hart, 2006), which further supports adding privacy concerns to the current study's theoretical framework. Dinev & Hart (2004) found the effect of risk-benefit calculus on privacy concerns to be higher than the effect of perceived control. Additionally, Malhotra et al. (2004) proved that concerns have an effect on risk beliefs.

The risk-benefit calculation of privacy calculus appears in all three previous models for perceived privacy: Adams (1999), Chang et al. (2018), and Dinev et al. (2013). And thus, privacy calculus seems to be a logical way to define perceived privacy risks and their influence on users' perceptions of privacy in this study. The privacy calculus theory was used in the interviews in the form of asking if and how the participant balances risks with the possible benefits when making a cookie consent decision. Additionally, the risk-benefit evaluation helped in better understanding users' disposition to value their privacy.

Privacy risks have been categorized by Dinev and Hart (2006) and Pavlou (2003). Dinev and Hart (2006) define two types of privacy risks: sharing information to third parties, and misuse of information (e.g., unauthorized access or theft). Pavlou (2003) categorizes risks into behavioral and environmental risks.

Behavioral risks – related to disclosing private information – can be economic risks, personal risks, seller performance risks, or privacy risks. Environmental risks are divided into economic risks, and privacy risks (Pavlou, 2003). Environmental privacy risks are defined by Pavlou as theft of private information or their illegal disclosure. The privacy risks by Pavlou (2003) are similar and could be divided into three simple risks: unauthorized access, theft, and sharing to third parties. These privacy risk categories were used as guiding keywords by the interviewer when conducting the interviews of this study.

To conclude, perceived privacy risks' influence on perceived privacy has been previously pointed out, and therefore it was added into this framework. The main way that privacy risks are taken into account in this study is through the privacy calculus theory.

4.4 Design's role in the framework

As the study's goal is to understand how deceptive design influences users' perceptions of privacy, a design-factor was added to the theoretical framework. It is looked at, how design – more specifically deceptive design – influences each of the four previously mentioned influencing factors inside the framework, as well as deceptive design's influence on the overall perception of privacy.

The connection between design and perception of privacy has not yet been confirmed, but there have been signs of their connection. For example, the Online Buying Persuasion model (OBP) by San Martín and Camarero (2009) shows that the website's design affects customer satisfaction, which in turn affects trust. And as it was shown earlier in the models by Chang et al. (2018) and Adams (1999), trust directly affects perceived privacy. Similar to the OBP model, a study by Lai (2016) shows that design affects the system's perceived usefulness and perceived ease of use, which translates to a person's motivation to use it. Additionally, Bélanger and Crossler (2011) found that design choices, such as transparency, could influence users' trust and privacy concerns. Lastly, as already mentioned in section 3.2. Privacy-protective design, multiple scholars have found design to have some kind of influence on users' privacy, as there has been a need to develop privacy-protective design guidelines.

The above-mentioned previous models and findings show that there is a connection between design and privacy, possibly also regarding users' perceptions of their privacy. In the design-related studies about privacy (introduced in section 3.2) deceptive design's specific influence on users' perceptions of privacy was not studied.

4.5 Previous research on users' perceptions of privacy in cookie consent requests and deceptive design

In this section, findings from existing literature about users' perceptions of privacy in the context of cookie consent requests and regarding deceptive design's influence are presented. Aligning with the overall findings from previous literature, Gray, Chen, Chivukula, and Qu (2021) have reported deceptive patterns to cause users to perceive a lack of privacy. Habib et al. (2022) have made a similar finding, stating that the poor usability of cookie consent requests, including deceptive patterns, can cause privacy fatigue in users - finding it exhausting to think about the consequences of internet use to their privacy - enhanced by the prevalence of encountering cookie consent requests. Likewise, Mathur et al. (2021) have found deceptive patterns to undermine and diminish users' privacy. Taking it further, Graßl et al. (2021) have demonstrated that a user's perception of privacy also affects their consent choice.

Next, the previous research is presented in relation to the four influencing factors for the perception of privacy: privacy concerns, control, trust, and privacy risks. It is important to note that no previous research has looked at the perception of privacy from a qualitative, user experience-oriented perspective, concluding with the overall perception of privacy, consisting of users' impressions and attitudes on the topic. Additionally, no previous research has shown how deceptive design influences the users' overall perceptions of privacy and its four influencing factors.

4.5.1 Perceptions of privacy concerns

When it comes to users' concerns about their privacy, Alharbi et al. (2023) have stated that privacy is one of the biggest concerns of users since websites started using cookies, with the main concern of users' being who has access to their data. Regarding privacy concerns, Gray, Chen, Chivukula, and Qu (2021) have found users to be the most concerned about the amount or the type of information that is being collected of them. The users in their study were also concerned about big data - they especially believed that the organization is using that data without permission only for their own benefit. The participants of a study by Bongard-Blanchy et al. (2021) were concerned about the potential risks that deceptive design could cause, although, the participants stated not to be generally worried about their privacy when deceptive design is used. Similarly, Mathur et al. (2021) reported users being concerned about the potential risks related to deceptive design. Lastly, a study by Ha et al. (2006) shows that users were concerned about the amount of effort needed for managing the cookie data collection.

4.5.2 Perceptions of control

Maier and Harr (2020) argue that users' control has an important impact to their privacy, since with control they can minimize any damage that the possible risks

of deceptive design might cause them. The participants in their study stated that paying attention and using the internet with caution - whilst remembering that not all parties always have the best interest of users in mind - they can protect their own privacy (Maier & Harr, 2020). Although, as the following existing literature shows, despite this idea of users, deceptive patterns do affect users' control. Control, in the current study, means the users' ability to make a consent choice that they want. Graßl et al. (2021) have suggested that depending on the deceptive pattern users' perception of control could decrease, but they stated that more research is needed to prove this connection. A study by Mathur et al. (2021) has shown that user's privacy could decrease when deceptive patterns are used to, for example, push the user toward spending more money than they intend, causing financial loss to the user. Forbrukerrådet (2018) and Graßl et al. (2021) have both concluded that some deceptive pattern types only create an illusion of control. Graßl et al. (2021) have exemplified that this can happen when the users are not given an option to decline their consent but rather a settings button, which at the end does not give the best possible control to the user.

4.5.3 Perceptions of trust

The literature on deceptive design's influence on perceived trust is extensive. Mathur et al. (2021) have reported that a user's consent choice is largely impacted by their trust in the website. In the same vein, Mejtoft et al. (2023) have suggested that the user's perceived initial trust is important for the long-term customer relationship with the service. Like Mejtoft et al. (2023) and Mathur et al. (2021), Nouwens et al. (2020) have stated that trust in the website or the data collector is a meaningful influencing factor for the users' consent choice. Mejtoft et al. (2023) have found that more trust often results in accepting all cookies, although they mentioned that deceptive design is more important than trust for the user's consent choice in a cookie consent request. Maier and Harr (2020) have reported users blaming organizations for using deceptive design and describing the data collectors as dishonest, resulting in deceptive design weakening their trust in the service. The users in a study by Lupiáñez-Villanueva et al. (2022) reported that deceptive design made the consent interface more difficult to understand and less transparent, decreasing their trust. As a reminder, Gray, Chen, Chivukula, and Qu (2021) have pointed out that trust could also be influenced by other things such as culture, although their study also found that deceptive design makes users more distrustful toward the service. Interestingly, a study by Lupiáñez-Villanueva et al. (2022) reported findings related to the users feeling sympathy toward the data collector by thinking that maybe the collectors do not use deceptive design on purpose, and that deceptive design is a natural part of doing business. A study by Kretschmer et al. (2021) has revealed the data collectors' side as well, reporting that the data collectors wish to increase their users trust in them by offering increased control.

4.5.4 Perceptions of privacy risks

Perceived privacy risks of deceptive design and cookie consent requests have been widely studied. Users have perceived the use of deceptive design to pose risks such as: being a victim of a crime (fraud, scam, virus, or hacking) (Bongard-Blanchy et al., 2021; Gray, Chen, Chivukula, & Qu, 2021), being lured to buy more and causing a financial loss (Bongard-Blanchy et al., 2021; Mathur et al., 2021), and a loss of self-confidence due to deceptive design making decision-making more difficult (Bongard-Blanchy et al., 2021). Ha et al. (2006) have reported that users see the potential risks to their privacy related to cookies, but they choose to do nothing about it and continue using the service as usual. Like Beckwith (2003), Flinn and Lumsden (2005) have suggested a possible explanation to this: the users' unawareness of cookies' purpose and function as well as data collection methods and their extent might lead to inappropriate conclusions about the privacy risks, thus making it impossible for the users to evaluate the privacy issues related to cookies or believing there are risks that do not actually exist. Therefore, Maier and Harr (2020) have suggested that users should be better educated on deceptive patterns to be able to recognize them and protect themselves from being deceived. Another reason for users' irrational behavior regarding the perceived risks might be, as suggested by Graßl et al. (2021) and Utz et al. (2019), that users do not function rationally but rather they tend to function heuristically in consent-giving situations, which is often contrary to the privacy calculus theory as well. Privacy calculus, an important theory related to privacy risks, has been assessed in previous research regarding deceptive design. The users in a study by Gray, Chen, Chivukula, and Qu (2021) functioned as privacy calculus suggests - balancing the perceived benefits with perceived threats when deciding to use the service. A study by Maier and Harr (2020) showed that deceptive design only benefits the organization, not the user - but still, the users would use the website despite deceptive design, indicating that there are not enough risks related to it compared to the benefits that the user would get from the service. The users in Maier and Harr's study (2020) identified financial profit and organizational growth as benefits for the organization.

5 RESEARCH METHODOLOGY

In this chapter, the research methods used in this study are introduced and it is presented how the study was conducted from recruiting the participants to shaping the interview themes to creating the mock-ups for the user tests, and to the data analysis. Additionally, the trustworthiness and methodological limitations of the study are considered, as well as the ethical aspects of conducting the study. Lastly, it is presented how artificial intelligence tools were used in this study.

The topic was approached from a qualitative perspective. There has been a lot of research on similar topics from a quantitative point of view, but instead of looking for statistically measurable answers, the goal of this study was to look for users' comprehensive perceptions on the topic, which is not equally possible with quantitative research. Hirsjärvi et al. (1997) also support the idea that quantitative methods are better for specific questions, and qualitative methods suit better when a more comprehensive look on the topic is desired. It is not desired to know "how much" or "how likely" users are to perceive cookie consent requests this way - the questions that this research wants to answer are "what", "how", and "why" users perceive it like they do. Next, the three different methods used in this study are introduced.

5.1 Triangulation of research methods: user testing, think-aloud, and thematic interviews

In triangulation, multiple methods are used to research the topic and collect data (Hirsjärvi et al., 1997). In this study, user testing, the think-aloud method, and thematic interviews were conducted to form a triangulation. Therefore, also the data consisted of multiple types of data: interview recordings, think-aloud recordings, and observations that were done during the user tests. This triangulated approach to the study was chosen to provide a comprehensive understanding of users' perceptions surrounding the topic, as triangulation has been proven useful especially in user experience research, allowing for the collection of richer

and more comprehensive data (Pettersson et al., 2018). Triangulation of methods and data was also chosen for this study since a similar approach was effectively used by Mejtoft et al. (2023) to study users' perspectives on cookie consent requests and the influence of deceptive design on their trust in the data collector. They combined surveys of attitudes related to cookie consent requests, user tests of organizational trust combined with the think-aloud method, and user tests of the cookie consent requests' design (Mejtoft et al., 2023). Similarly, The Interaction Design Foundation (IxDF, 2016) recommends balancing semi-structured interviews with user testing, to ensure a comprehensive understanding of users' needs and preferences. Likewise, Tan et al. (2009) state that a combination of multiple methods - such as usability testing and heuristic evaluation - might work better for a more comprehensive understanding. Lastly, triangulation of methods was chosen because it adds to the trustworthiness of the study (Hirsjärvi et al., 1997).

The first method chosen for this study is user testing, with which it is not only possible to observe the design's functionality but also to capture users' subjective impressions and perceptions of it. It is mainly a usability evaluation method that focuses on understanding usability issues based on the experiences and feedback of actual users as they complete specific tests within a specific use scenario (IxDF, 2016; Tan et al., 2009). User testing is a closely related method to usability testing, and some people even use these two terms interchangeably (IxDF, 2016). With user testing, it is possible to catch users' perceptions, values, and experiences on a topic, while usability testing mainly focuses on users' ability to use a service and their satisfaction while using it (IxDF, 2016). Similarly, Tan et al. (2009) found that user testing, in comparison with heuristic analysis, is especially useful in capturing users' real experiences and satisfaction, not only usability issues. IxDF (2016) recommends asking users to think aloud during user testing. Due to their recommendation, and the earlier mentioned study conducted by Mejtoft et al. (2023), think-aloud was considered a complementary method alongside with the user testing. The think-aloud method requires the participants to talk aloud their thoughts, decisions, and reasoning processes as they use the interface, as if they were talking aloud to themselves (Jørgensen, 1990). In this study, it was desired that the users would describe their thoughts and feelings of deceptive patterns in the cookie consent request's interface while using it themselves. Jørgensen (1990) has interviewed system designers who have used this method in their design processes, and their study shows that the think-aloud method has been successful in user interface design research previously. The think-aloud method can reveal design issues that might not be immediately visible (Jørgensen, 1990), possibly making it a suitable method for revealing users' perceptions of privacy, since perception of privacy is not a thing that a designer can always visibly notice themselves.

To add to the depth of the study, semi-structured thematic interviews were conducted after the user testing. This method, as described by Hirsjärvi and Hurme (2017), allows for exploring topics through flexible and open-ended discussions centered around specific themes rather than a set of rigid questions.

According to Merton et al. (1956, as cited in Hirsjärvi & Hurme, 2017), this method allows participants to freely discuss their past experiences in a natural interview setting that encourages the participants to give rich and individualized answers. Thematic interviews align well with the study's goals, offering flexibility for the participants' answers which respects their boundaries since privacy can be a sensitive topic to some. Furthermore, Eccles and Arsal (2017) have stated that combining interviews with the think-aloud method can reveal new insights of the topic, meanwhile complementing the data gathered in user testing. The interviews would provide perspectives that expand beyond the findings related to the task-related impressions from the user testing. Thus, thematic interviews support and enrich findings from the other methods, offering a more comprehensive understanding of users' perceptions, as also suggested by Hirsjärvi and Hurme (2017).

Prior to the research setting, participants completed a short survey through Webropol to gather their demographic information in order confirm that they have lately encountered a cookie consent request and to ensure that they belong to the specified demographic group. Participants also received an information leaflet and a privacy notice stating the study's purpose, procedures, and data handling practices. This also reduced the time needed for any preliminary questions in the interview itself. The participants were not briefed on the specific interview themes beforehand, as it was not necessary for them to prepare for the interview. This kept the interview setting relaxed but professional, creating a setting for honest and confident responses.

Lastly, a slightly phenomenological standpoint was intentionally taken in the interviews. The goal of a phenomenological interview, as introduced by Perttula (1995), is to raise the participants' awareness of the topics of the study, for them to be able to better communicate their perceptions and impressions of them. Through a phenomenological interview, it is possible to capture participants' perceptions, experiences and thoughts on how or why the participants perceive the topic the way that they do (Perttula, 1995), which is important regarding the first research question of this study: how and why the participants perceive the privacy when deceptive design is used. The goal of the interviews was not to be fully phenomenological, as one of the goals of a phenomenological study is for the interviewee and the interviewer to come to a conclusion of the answer together (Perttula, 1995). Instead, the interviewer's goal in this study was to stay neutral to the topic throughout the study. The phenomenological aspect can be seen in this study as an educational goal to help the participants understand the topic better and thus give more realistic answers within the themes, compared to not understanding the topic at all.

To summarize, these three methods (user testing, think-aloud method, and thematic interviews) all contribute to understanding the complex and broad concept of the perception of privacy. With data triangulation, the research questions can be answered more comprehensively, giving more trustworthiness to the findings. Next, the practical application of these methods is presented.

5.2 Conducting the study

This section introduces the practical steps taken to implement the study's triangulated research methods. First, a literature review was conducted to find out what has already been researched, with which methods and concepts, and what kind of gaps there are in the existing literature. Literature was searched from Google Scholar, JYKDOK, IEEE Xplore Digital library, and ACM Digital library with a combination of keywords such as privacy, cookies, cookie consent, user experience, perceptions, perceived privacy, dark patterns, deceptive patterns, nudging, and deceptive design. The literature review formed the theoretical framework for the study.

After the theoretical framework was formed, the data was collected through a triangulation of research methods: user testing combined with the think-aloud method, followed by a thematic interview. Each of the three methods was conducted consecutively in a single session with one participant at a time, via Microsoft Teams. This individual setting was chosen to focus on personal and individual perspectives, since they were central to answering the research questions. The entire process, from the beginning of the user testing combined with the think-aloud method to the end of the interview, was recorded using Microsoft Teams - both audio and screen. The structure for the research setting, including instructions for the user tests and the interview themes and questions, can be found in appendix 1.

Before moving onto the official research, the methods were tested with one person to see if the mock-ups and interview themes work as they were intended to, as Hirsjärvi et al. (1997) have also suggested to do regarding interviews. The test round allowed for checking for any technical issues, and it gave the possibility to add, edit or remove content from the user tests and the interview. Only minor adjustments needed to be done to the interview questions and some edits needed to be done to the functionality of the user tests' mock-ups after the test round. The test round additionally helped to more accurately estimate the time needed for conducting the research sessions.

In the following subsections, the recruitment process and the selection criteria for the participants are explained, followed by a description of the process for creating the mock-ups for the user tests. Then, the practical application of the research methods is presented, including the specific procedures used to conduct the methods.

5.2.1 Participants and recruitment

Choosing the participants was done by carefully selecting the target group and not with a random selection, as Hirsjärvi et al. (1997) suggest for a qualitative study. The participants were invited to the study via e-mail with invites sent to different faculties e-mail lists in the University of Jyväskylä. A visually attractive digital poster of the invite was also created and shared to different online platforms and communities (e.g. Facebook groups and Discord servers of the

researcher's personal interests), expanding the possibilities of getting people from different backgrounds and technological preferences to participate in this study.

The criteria for participating in the study were as follows. The participant should be a university student either completing their Bachelor's or Master's studies. Additionally, the participant should be a part of the generation Z, more specifically a person born between the mid-1990s to early 2010s. The age group was chosen because they grew up during a rise of technological development and are often referred to as "digital natives". Known for their tech-savviness and quick adaptability to new technologies, Generation Z university students were considered suitable for this study since they may share similar perceptions, which possibly helps in unifying the results of the study.

Although it would have been ideal to conduct the interviews until saturation was achieved (as suggested by Hirsjärvi et al., 1997), this approach was not reasonable for a master's thesis due to its time constraints and the limited experience in recognizing saturation. Instead, eight participants were selected for the study, as recommended by the thesis' supervisor and as it has been a common amount in similar master's theses. The number of participants chosen for the study seemed to provide an informative amount of data to support the research questions, especially since the research settings were time-consuming and the amount of data per participant was extensive. Additionally, it was found challenging to get people to want to participate in the study due to the long duration of the research sessions.

Participants' demographic information was removed from this thesis, as it did not bring interpretive value to the findings, due to the study's limitations. One limitation of this study was the limited time available for analyzing the participants' perceptions based on their demographics. Therefore, the data was analyzed as applying to one demographic group only, not separating any results between the different, more specific, demographic details. The demographic information was only collected in a general sense to capture a certain demographic group's perceptions, and the demographics did not influence the interpretation of the results. However, an overview of the general demographics of the participants is next presented to enhance transparency. The demographic information of the participants' varied, reflecting a variety of perspectives within the criteria that there were for the participants' recruitment (age and educational level).

The average birth year of the participants was 1998, with years ranging from 1995 to 2002. The gender representation was 63,5% female, 25% male, and 12,5% other. Additionally, 62,5% of the participants were studying at the bachelor's level and 37,5% were studying at the master's level. The participants represented a variety of academic fields: information technology, humanities, arts, education, health and wellbeing, natural sciences, and economics. This variance possibly added depth to the findings of this study. The participants' mother tongue or nationality was not inquired, but seven of the research settings were conducted fluently in Finnish and one fluently in English.

To protect the confidentiality of participants' data, each participant was given a code to differentiate their answers from each other. The participants' codes are simple, ranging from P1 to P8, where "P" stands for "participant" and the number is assigned randomly from 1 to 8.

5.2.2 Creating mock-ups for user testing

Instead of using actual websites and their cookie consent requests for the user testing, self-made mock-ups were used in this study. Mock-ups were used instead of actual cookie consent requests to avoid the influence of the website's brand on users' perceptions, which is a known factor in shaping user experience (Brakus et al., 2009). This could have interfered with the study's focus on privacy. It was also not desired to have the users share their cookie data with actual websites for the sake of this study and therefore, mock-ups were a more privacy-protective option in that sense.

The mock-up user interfaces for the cookie consent requests were created in Figma. Three different mock-ups were used with three different types of cookie consent request styles and a combination of several different deceptive patterns. The cookie consent request styles were amongst the top 5 most common cookie designs found by Singh et al. (2022), Alharbi et al. (2023), and Kretschmer et al. (2021). The mock-ups were designed based on the most common deceptive patterns found in previous research, as introduced in subsection 2.2.1 Deceptive design elements: deceptive patterns. The selected deceptive patterns were not only the most common ones but have also been suggested to possibly lead to unintentional data disclosure or would be illegal regarding the current cookie legislation - such as Habib et al. (2022) have done in their mock-ups. The cookie consent request styles and deceptive pattern types are presented more closely in chapter 2, and therefore, they are not cited in the following descriptions of the mock-ups.

The first mock-up is a binary choice between accepting or declining cookies, with only a short text explaining the practical information related to cookie data collection. The first mock-up is illustrated in the following figure 2, and bigger pictures of each step of this user test can be found in appendix 2. At least four deceptive patterns were intentionally used in this mock-up. First, misdirection was used to purposefully try to turn the user's focus on the bigger and more colorful "accept" button to distract their attention from the less visible decline-option. Second, visual interference was used to disguise the decline button from looking like a clickable option. It was made to look like it is not a button, but rather it looks like a piece of unimportant text. Third, forced action was used by including an X button in the corner of the consent request to make it look like the user could bypass the request by clicking it, but in reality, clicking the X informs the user that it is not possible to do that and instead they are forced to make a consent choice, which is an undesirable action for the user whose intention is to bypass the request. Lastly, confirmshaming was used in the decline-option's text by making it emotionally manipulative to try to get the user to steer away from that option, since it would give the user "a bad user experience" on the website.

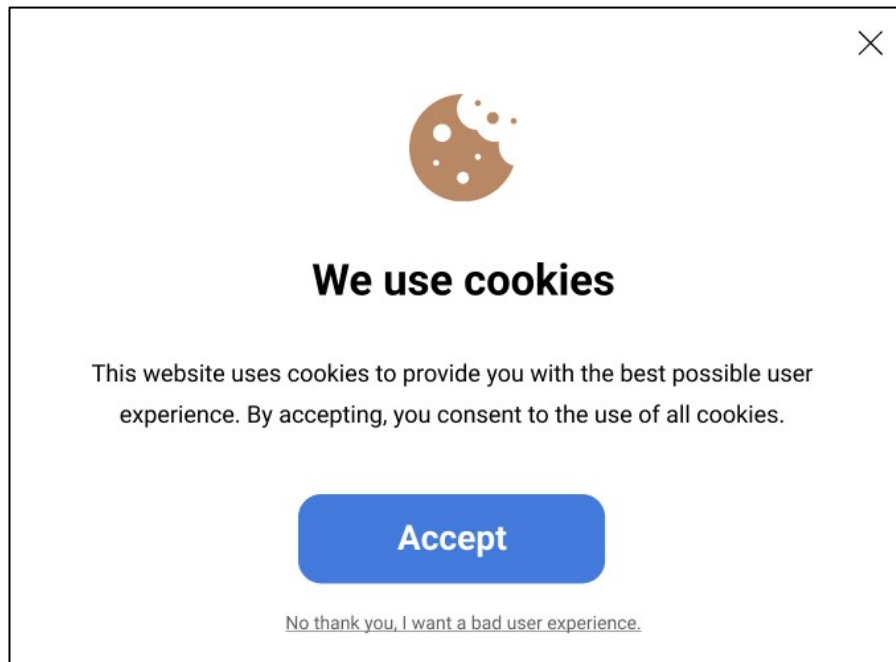



FIGURE 2 The first cookie consent request mock-up used in user testing

The second mock-up is an informational cookie interface. This mock-up had a little bit more text and an option to go read more about the website's privacy policy and cookie data collection. The consent options in this mock-up were to "accept all cookies", or to go to settings, which opened up a bigger consent request including different types of cookies to select from. The second cookie consent request mock-up is presented in the following figure 3, and bigger pictures of each step of this user test can be found in appendix 2. At least five different deceptive patterns were intentionally used in this mock-up. First and most visibly, misdirection and visual interference were used, similar to the first mock-up. Regarding the visual interference, the settings-option is a disguise, since it does not specifically state what the settings are related to and if through the settings it is possible to also decline consent. Similarly, the settings page made the "accept all"-option more appealing and visible to the user instead of highlighting the "save settings"-option. Then, the settings page included forced action when the user tried to decline the collection of essential cookies, because it was designed to look like it was a possible option. The error message that pops up when trying to decline the collection of essential cookies is also called nagging, which means that the user tries to complete a task but is persistently interrupted by requests to do something else that is not in their best interest. Lastly, similar to the first mock-up, confirmshaming was used in the text to make it seem like accepting all cookies would benefit the user more than declining them. Additionally, in this second mock-up, there was no direct option to decline cookie data collection, other than by clicking "save settings" with only the collection of essential cookies turned on.




We use cookies

On this website, cookies are used to ensure the functionality of the website, for statistical and analytical purposes, and to personalise content and marketing. By accepting all cookies, you ensure the functionality of the site and the best user experience. You can change your cookie preferences in the settings.

[Read more about privacy policy and cookies.](#)

[Settings](#) [Accept all](#)

FRAME 1: start



Cookie settings

- Essential cookies**
 These enable functionalities that are essential for using the site, such as logging into secure parts of the site, remembering the contents of your shopping cart in online shops, filling in forms or improving security.
- Functional cookies**
 These cookies are used to enhance and improve the functionality of the website, but they are not strictly necessary to use the site.
- Personalization cookies**
 These cookies make it possible, for example, to remember the choices you make on a page, such as language and font size, or your username and password between visits to the site.
- Marketing cookies**
 For example, these cookies can be used to collect information about your interests based on your online behaviour and to show you targeted advertisements based on this information.

[Read more about privacy policy and cookies.](#)

[Save settings](#) [Accept all](#)

FRAME 2: settings

FIGURE 3 The second cookie consent request mock-up used in user testing

The style of the third cookie consent request mock-up is called cookie categories (also known as multiple-choice banner or numerous options banner). The third mock-up can be seen in the following figure 4, and bigger pictures of each step of this user test can be found in appendix 2. At least three deceptive patterns were intentionally added to this mock-up. First, preselection was used by introducing all cookie types for the data collection as preselected options. Comparison prevention is another deceptive pattern that can be seen in this mock-up, although, it is not an extreme example of the pattern. With comparison prevention, many options are presented to the user in a complex and hard-to-understand manner, possibly making it difficult for the user to compare the different cookie data types for making a consent choice. Additionally, misdirection regarding the imbalance between accepting all cookies and saving settings can be seen in the mock-up. Lastly, the third mock-up did not include a simple option to decline consent.

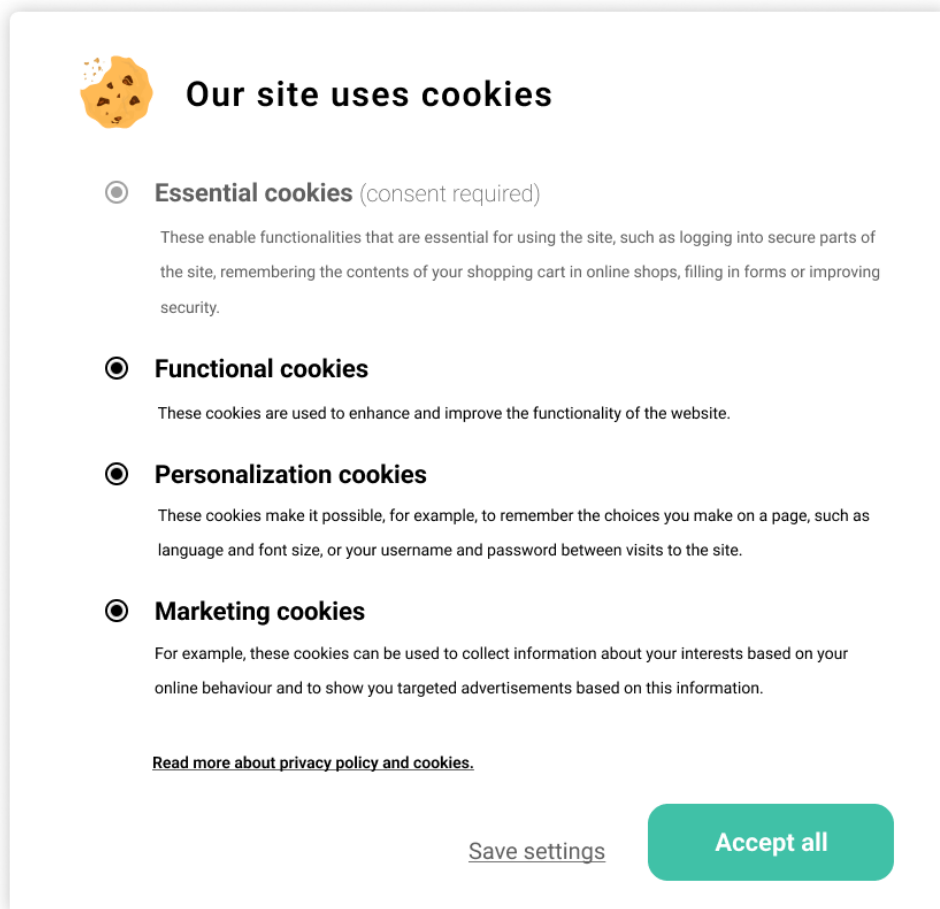


FIGURE 4 The third cookie consent request mock-up used in user testing

All of the mock-ups blocked the user's access to the website before making the consent choice, which was intentionally done so that the participant of this study would have to complete the request and to have to think about its design. If they were able to enter the website without making a consent-choice, the user testing would have been meaningless. In reality, blocking the users' access to the website before making a consent choice is a type of deceptive pattern called obstruction. Additionally, the second and third mock-up included a deceptive pattern called sneak into basket, where the user is guided toward accepting all cookies instead of saving their selected cookie category settings – this pattern sneaks both non-essential and essential cookies into the data collection, as the user might mistakenly click on accepting all even if they had chosen other types of cookie categories to consent to.

The mock-ups used in the user testing were high-fidelity, meaning that they provided a realistic representation of a cookie consent request. This enabled as natural setting as possible for the research, which Hirsjärvi et al. (1997) state to be a characteristic of qualitative research. The mock-ups were fully functional regarding the interactive elements (such as buttons and options to choose from), closely simulating the reality, and enabling participants' comprehensive feedback on the features and the overall perceptions of the deceptive patterns. When the user had made a consent choice, they were able to enter a mock-up website.

5.2.3 Conducting user testing with the think-aloud method

To introduce the participants to the topics of the study and prepare them for the interview, user testing was conducted in combination with the think-aloud method. The cookie consent request mock-ups functioned as a warm-up to the topics, giving visual examples to the participants of how deceptive patterns and cookie consent requests commonly look like. The user testing consisted of three user tests, in which the three mock-up interfaces were used. The tasks were simple: the participants only needed to make a consent choice in order to complete the mock-up cookie consent request.

The think-aloud method, as recommended by Eccles and Aarsal (2017), involved instructing participants on how to verbalize their thoughts while interacting with the mock-ups. Following the guidelines of Eccles and Aarsal (2017), the participants were instructed to talk aloud everything that they would say or think to themselves as they performed the test, acting as if they were alone in the room and talking to themselves. Whenever the participant was not actively thinking aloud, they were reminded to do so, as instructed by Eccles and Aarsal (2017). To ensure participants' familiarity with the think-aloud method, the participants first conducted two to three warm-up user tests on external websites (e.g., University of Jyväskylä and the Finnish National Cyber Security Center), as also suggested by Eccles and Aarsal (2017).

Observing the participants' actions during the user tests allowed for understanding their cognitive processes related to the topic, which aligns with the idea by Hirsjärvi et al. (1997) that observational methods in qualitative research allow for seeing a difference between how the participants' act in reality compared to how they say that they normally act. Therefore, combining both listening (think-aloud) and observing (user testing) is crucial for getting comprehensive results. Additionally, it was noticed that the participants found the user tests useful when expressing their thoughts in the interview, as the tests allowed for them to use specific parts of the mock-ups as examples.

Each user testing session was conducted online via Microsoft Teams, as it is an easy way to simultaneously record audio, video, and screen. These three types of recordings were necessary for capturing the participants' reactions, interactions, and comments. The participants were informed that they could choose to turn off their video for privacy and comfort, but the screen was still recorded to capture the user tests for easier understanding of the references made about them in the audio recording.

5.2.4 Conducting thematic interviews

Thematic interviews were conducted to gain deeper insights into participants' experiences, impressions, attitudes, and perceptions of privacy regarding each of the influencing factors (privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks) from the theoretical framework. This semi-structured interview method was chosen due to its flexibility, as it allows for discussing specific themes while encouraging participant-led responses that

genuinely reflect the participant's perceptions. Thematic interviews aligned well with this study's goal of understanding the participants' perceptions, impressions, and attitudes of privacy in-depth.

Each research setting began with introductory questions about the participant's general views on privacy, their awareness of privacy issues, and their previous experiences with deceptive design and cookie consent requests. These preliminary questions prepared the participants for the user testing, which was followed by the thematic interview itself. Additionally, the beginning of the research setting followed the phenomenological aspect of this study - the participants were asked to freely explain their understanding of the concepts of privacy, cookies, and deceptive design, and if they were unsure what the concepts meant, they were more closely introduced to the participants.

The interview themes directly arose from the theoretical framework for the perception of privacy introduced in chapter 4. The themes included privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks. Additionally, a theme related to design was included. These five themes guided the discussion but allowed for the participants to flexibly share their thoughts and expand on relevant topics. The themes, as advised by Hirsjärvi and Hurme (2017), were addressed in a flexible order following the participants' answers and based on what the discussion was steering toward. But when the conversation started to go off-topic, the interviewer guided it back to the relevant theme at hand, as suggested by Hirsjärvi et al. (1997). With these, a balance was maintained between participant-led responses and focus on the topic.

Each theme was structured with guiding questions that were inspired by previous research and theories related to the influencing factors for the perception of privacy. For example, IUIPC and CFIP scales helped to identify users' privacy concerns, meanwhile FIPs principles and the different levels of trust helped in understanding the participants' trust in the data collector. Likewise, the privacy attributes introduced by Barth et al. (2022) were used to identify deceptive design's influence on the privacy perceptions of certain design elements. Additionally, the privacy calculus theory was used to understand the way that users' trade their privacy for possible benefits. More examples of the guiding questions and keywords can be found in section 4.3 Influencing factors within the framework. The guiding questions supported the interviewer in covering essential topics inside the themes without limiting the flexibility of the conversation and its natural adaptation to the participants' answers. An outline of the interview themes and questions can be found in appendix 1.

Each theme was discussed in the light of deceptive design's influence on the users' perceptions. Regarding each theme, users' previous experiences, opinions, and general impressions on the topic were highlighted. At the end of the interview, concluding thoughts of the whole research setting were discussed.

Microsoft Teams was used to conduct and record the interviews, recording audio, video, and screen for further transcription of the data. Participants could choose whether to have their camera on for privacy reasons, but all participants

preferred to have it on for a more authentic conversation. The video recording allowed for better referencing to specific interactions during the transcription.

Overall, the thematic interview method allowed for flexibly and comprehensively explore the complex topics, as well as complemented the observations from the user testing. By carefully selecting the interview themes and their guiding questions and keywords, the interviews ultimately provided a comprehensive understanding of participants' impressions and perceptions.

5.3 Data analysis

This section introduces the overview of the data including its length in pages, and the way that the transcriptions were done. Additionally, it is explained how the data was analyzed with thematic and content analysis methods.

5.3.1 Data overview

The preliminary transcription for the user tests, think-alouds and interviews was done automatically by Microsoft Teams to a Microsoft Word document when the research settings were conducted. The whole preliminary transcription was then proofread and corrected, since it was not fully accurate due to the automatic transcription having made mistakes in what it heard. The transcription was written word to word, as suggested by Hirsjärvi and Hurme (2017), but sighs and bodily expressions were left out for the most part, if they did not seem relevant to the interviewee's commentary. This, as instructed by Hirsjärvi and Hurme, was an applicable technique, if only one person was going to analyze the data and would be very familiar with the interviews and the topics of discussion. Any parts of the transcription that could identify the participant (such as names, places, or places of work) were left out of the final transcription, and visually the transcriptions followed Hirsjärvi and Hurme's (2017) general instructions. The transcriptions were written in the original language of the research setting with the participant (either English or Finnish, as stated in subsection 5.2.1 Participants and recruitment). After the data analysis, when introducing individual quotations of the participants in chapter 6 Results, the quotations were translated to English if they were not in that language originally.

The total duration of the recorded interviews and user tests was 14,7 hours or 882 minutes. The research settings' durations varied between 93 and 130 minutes, with the average duration being 110 minutes. The total length of all transcriptions was 513 pages, while an individual transcription of one participant varied between 57 to 77 pages, with the average length of the transcriptions being 64 pages. The transcriptions were written with the Aptos font (size 12) and a line spacing of 1.1 in Microsoft Word.

Lastly, the user testing, think-aloud method, and interview were a cohesive and unified research setting, in which the discussion happened naturally and flexibly throughout the whole setting. The discussion sometimes overlapped

between the themes and the user tests, and jumped from one point to another, making it difficult to separate these research settings from each other. Therefore, the data from each participant was also transcribed into their own singular text file without separating the methodological approaches from each other. This is why the data from the user testing, think-alouds, and interviews were not analyzed separately, but rather as a whole. Moreover, the quotations in the following results chapter are not specified regarding the different data collection methods, as all data were considered a part of one unified whole. But to mention, the data from each part of the research (including user testing, think-alouds, and interviews) were utilized in the analysis, making each of the methods important to the research findings.

5.3.2 Analysis process

The analysis was conducted by combining thematic and content analysis and utilizing the influencing factors from the theoretical framework as well as the initial research questions as a guideline. The four influencing factors were not used as measurable variables in this study.

Thematic analysis, according to Braun and Clarke (2022) is “a method for developing, analyzing and interpreting patterns across a qualitative dataset, which involves systematic processes of data coding to develop themes” (p. 4). Content analysis instead, according to Tuomi and Sarajärvi (2002/2018) is a broader method that applies to all types of qualitative research due to its flexible framework, making it compatible with other data analysis methods. In this study, the framework for content analysis by Tuomi and Sarajärvi (2002/2018) was used, combined with the structural guidelines for thematic analysis defined by Braun and Clarke (2022). First, coding, theme identification, and theme refinement were conducted following Braun and Clarke’s guidelines, and then, the themes were further synthesized and categorized according to Tuomi and Sarajärvi’s approach.

The thematic analysis began during transcription, with preliminary ideas emerging from the data. Initial observations, as instructed by Braun and Clarke (2022), were written down, which allowed for early identification of themes. Since the beginning of the data analysis, the goal of the study - more specifically the research questions - were kept in mind, as suggested by Tuomi and Sarajärvi (2002/2018). This was helpful when looking for possible codes and themes that aligned with the research questions. Braun and Clarke’s (2022) guidelines emphasize that the data familiarization process should be flexible, allowing for the themes to shift based on new insights found in the data, as it happened in this study when certain pieces of data suggested modifications to the research questions.

After the transcription, systematic coding was conducted based on Braun and Clarke’s (2022) instructions for generating initial codes. The theoretical framework’s four influencing factors (privacy concerns, control over privacy, trust, and perceived privacy risks) as well as design were used as primary codes, within which new codes appeared one by one as the data was systematically and

iteratively read through. The coding was implemented using a colored highlight tool on a PDF document, using a specific color for similar codes.

For content analysis, Tuomi and Sarajärvi's (2002/2018) guidelines suggest moving the relevant, coded parts of the data into another file for clarity. In this study, Microsoft Excel was used as a place to store these pieces of data. The codes that were moved to the Excel sheets always included the participant's code, the piece of text and its identifying code, and the possible theme related to it. As suggested in Tuomi and Sarajärvi's framework, the coded data was further sorted into separate sections representing different interests related to the research questions. In this study, three Excel sheets were used for organizing the data into: 1) perceptions of privacy without deceptive design, 2) influence of deceptive design on privacy, and 3) impressions of deceptive design and the cookie data collector. In the Excel sheets, non-essential content was removed, merged with similar content, and moved around to group similar content together. This step helped to identify any gaps in the collected codes, making it easier to look for further supportive codes in the original dataset. The Excel sheets also simplified and shortened the analysis of the large dataset of 513 pages.

During the systematic categorization of the data in the Excel sheets, Braun and Clarke's (2022) guidelines for theme identification were followed. The initial codes that were moved to the Excel sheets were carefully reviewed and then grouped together with similar codes, such as it was instructed by Braun and Clarke. An example of a pair of similar initial codes could be "incapable data collector" and "lack of professionalism", both signifying the participants' impressions of the cookie data collectors, which were further related to the participants' trust in them. Next, still following the guidelines by Braun and Clarke (2022), the grouped codes were more closely examined for broader patterns that related to the research questions, forming themes. For example, the codes "uncertainty of the use of cookie data" and "non-transparent data collection purposes" were grouped together and later categorized under a theme of "suspiciousness", referring to the participants' suspicions raised by deceptive design about the website's reasons for collecting cookie data. The grouped codes started to form initial themes, and as the codes were iteratively reviewed, as suggested by Braun and Clarke (2022), the themes became more refined. As the understanding became deeper, it became easier to identify patterns, and further identify themes.

After the data was moved to the Excel sheets, the original dataset was still revisited during multiple iterations because Braun and Clarke (2022) recommend that type of approach to thematic analysis. When revisiting the dataset, any new findings were added to the Excel sheets. This ensured comprehensive theme refinement. The themes were further reviewed in the Excel sheets to find any patterns in the data, and repetitive responses were also quantified to show a specific theme's prevalence among the participants' responses.

After the themes were formed, Tuomi and Sarajärvi's (2002/2018) content analysis framework was followed for synthesizing and categorizing the final themes, and concluding the final thematic findings related to the research questions. First, as suggested by Tuomi and Sarajärvi, the themes were synthesized

by organizing and grouping similar themes together. The data synthetization ended in the final categorization of the grouped-up themes. In their guidebook, Tuomi and Sarajärvi (2002/2018) suggest dividing the final themes and theme categories into subclasses and upper classes, which was also done in this study to ultimately form the results of the study. Examples of such subclasses could be “difficulty of understanding”, and “complicated”, which in turn formed an upper class of “diminished control”. During this synthetization and categorization process, special attention was put on aligning the findings with the research questions, as Tuomi and Sarajärvi (2002/2018) suggest doing since the beginning of the data analysis process. Finally, the structured themes and their categories could be considered the results of the study, which allowed for further discussing the findings and making conclusions of them regarding the research questions. Although, as it was already suggested by Hirsjärvi et al. (1997), it was difficult to let go of the data analysis process as a beginner researcher, because it was not simple to recognize when the data was analyzed thoroughly enough. Here, the time restrictions of the thesis helped to move on in the research process.

An important thing to note is the thought process behind looking for answers to the research questions. The influence of deceptive design on the perception of privacy was examined in relation to its four influencing factors: privacy concerns, control over privacy, trust in the data collector, and perceived privacy risks. Regarding each influencing factor, deceptive design’s influence on it was looked for in the data. It was then concluded how deceptive design overall influences each influencing factor. For example, if the participants perceived there to be more privacy risks related to cookie consent requests when deceptive design was used, it was concluded that deceptive design increased the perceived privacy risks and thus, the perception of privacy was considered to be more negative. When answering the research questions, deceptive design’s influence on the perception of privacy was concluded as either positive or negative, or something in between. Positive perception reflects a privacy-protective outcome, whereas a negative perception reflect that the users’ privacy is undermined or intruded. The middle ground was described as neutral or something else, depending on the participants’ conclusive perceptions. A neutral perception could have meant that privacy mechanisms are necessary and in place but they are not impactful to the users’ perceptions. Similarly, the users’ overall perceptions of their privacy were concluded as protected, respected, compromised, undervalued, or unimpacted.

5.4 Ethical and privacy considerations

In this section, the ethical and privacy considerations of the study are introduced. Ethical and privacy aspects are central to the foundation of the study. According to Kvale (1996), the first ethical consideration of a study is to validate the purpose of the study, with practical and theoretical contributions taken into account. In this study, a literature review was conducted and a theoretical framework was created for having a solid ground and for having a genuine research purpose.

The participants were informed about the study's purpose, procedures and any potential risks or benefits related to it, as instructed by Hirsjärvi and Hurme (2017). This was done by sending the participants an information leaflet and a privacy notice via email prior to the study. Additionally, the participants were sent a Webropol survey through which the informed consent of a participant was collected, which, according to Kvale (1996) is an important step regarding research ethics. The participants consented to the recording and analyzing of the research setting. It was fully voluntary for the participants to partake in the study, and they had the right to withdraw from it at any point without repercussions, as they were instructed in the information leaflet. Additionally, the possible benefits and risks for the participants were considered and shared with the participants in the information leaflet, as guided by Kvale (1996). Although no risks were expected from this study to the participants, and the main benefit for the participants would be to learn more about the topic and possibly be able to act more privacy-cautious on cookie consent requests afterwards. The information leaflet and privacy notice are attached to the end of this thesis (see appendices 3 and 4). Additionally, the participants were given a possibility to ask questions and express concerns regarding the study and their participation before, during, and after the research sessions were conducted with them.

The participants' data was handled confidentially and according to the GDPR (Regulation 2016/679). Additionally, the participants' personal information was either completely deleted or anonymized in the transcripts, per ethical and privacy guidelines. All data containing the participants personal information - including the demographic information collected through Webropol as well as the recordings - were deleted as the study was finished. The data was stored in Microsoft OneDrive (provided by the University of Jyväskylä) and the researcher's personal computer for a back-up. Access to both is secured with a password and OneDrive also has a two-step authentication process adding to the security. It was made sure that the data protection settings on the researcher's computer were up to date at all times. Additionally, the researcher was and is obliged to remain silent to respect the confidentiality agreed with the participants, as guided by Hirsjärvi and Hurme (2017).

The conduction of the transcription plays another important role regarding correctness, and thus, the ethicality of the study (Kvale, 1996). The transcriptions of this study followed the participants' answers word to word, with only bodily expressions and sighs left out, authentically capturing the participants' perspectives without unnecessary interpretation by the researcher. Additionally, the thesis is written in such a way that the participants won't be recognizable from the text, as instructed by Kvale (1996).

Deception and privacy can be considered sensitive topics by the participants, such as it was noticed by Maier and Harr (2020). Although, Maier and Harr stated there to be no problem with the sensitivity of the topic in their study, as long as the questions were asked neutrally, avoiding guiding the participant's answer to a certain direction or pressuring them. Maier and Harr (2020) also

added that the researcher's passive and neutral presence also helps the participants to freely share their thoughts without expectations or pressure. In this study, some participants perceived the nature of the study as therapeutic, and as deceptive design as a topic made the participants feel anger, frustration, and other negative emotions, it sometimes caused the participants to direct their emotional release toward the interviewer. This outcome is a common occurrence in interviews (Hirsjärvi & Hurme, 2017), but the interviewer in this study tried to maintain neutrality despite it.

The researcher attempted to maintain objectivity throughout this study, as it is a guiding principle in doing research (Hirsjärvi et al., 1997). During the interviews, as instructed by Brenner (1981, as cited in Hirsjärvi & Hurme, 2017), the researcher's personal opinions were left out and it was attempted not to guide the participant's answers to any direction, maintaining a participant-led discussion. The participants were not pressured to answer the questions neither, if they did not want to, as instructed by Hirsjärvi and Hurme (2017). Still, all themes were discussed comprehensively by the participants. Furthermore, the data analysis was conducted as openly and honestly as possible, taking all viewpoints and perceptions into account, without unnecessary generalizations, as Kvale (1996) also suggests. It was tempting to only look at the negative perceptions due to the negative association with deceptiveness, but conscious effort was made to avoid this.

Despite efforts to remain objective and neutral, it was found to be challenging at times, as the findings from the literature review had given the researcher an idea of what kind of results or answers might be expected, especially regarding deceptive design's negative associations. Lastly, as Hirsjärvi and Hurme (2017) point out, a qualitative study conducted with interviews is always a result of the participant's and the researcher's interaction with each other, where the persons participating in it will evidently influence the outcome.

5.5 Trustworthiness and methodological limitations

In this section, the study's trustworthiness and methodological limitations are discussed. Regarding qualitative research, the trustworthiness of the study, rather than its reliability or validity, is discussed (Eskola & Suoranta, 2014; Hirsjärvi & Hurme, 2017). The trustworthiness of a qualitative study mainly consists of four dimensions: credibility, transferability, dependability, and confirmability (Tuomi & Sarajärvi, 2002/2018). Next, these four aspects are presented regarding the current study.

Regarding the credibility of the study, the participants expressed it to be important for them to be educated on the topic, as it was then easier to discuss these complex topics, making them more engaged in the discussion. On the other hand, some participants seemed to be uninterested in talking about their privacy at times due to their overall anxiety surrounding their internet use and the uncertainty about their privacy. This sensitivity could have limited the true depth

of these participants' responses. Additionally, the credibility of the study was attempted to be improved, as advised by Hirsjärvi and Hurme (2017), by following the guidelines for data analysis and transcription unchanged from the beginning to the end regarding each participant's data. Additionally, as suggested by Hirsjärvi and Hurme, the recording tool's and the research setting's functionality was tested and made sure that they worked similarly each time. In this study, a test round of user testing, think-aloud and interview was conducted, confirming the settings of the Microsoft Teams tool. In case the participant's sound or screen sharing was not working properly, the interview was paused until the problem was fixed. For the most part, the research settings had no technical issues.

The transferability of the results is limited due to the study's focus on a specific demographic group (generation Z and university students) and a specific context (cookie consent requests). Although the sample size was broad for a very limited study like a master's thesis, the sample was still too small in order to generalize the findings to a broader group of users. Additionally, the context limitations do not allow for generalizing the results regarding other contexts, such as privacy policies. Furthermore, the study's theoretical framework in its current shape may not be directly transferrable to other contexts.

When it comes to the dependability of this study, the findings are not always fully dependent on the participants' viewpoints, but rather they are produced in the interaction between the participant and the researcher, acknowledging that undoubtedly the researcher's own perceptions and presumptions always subtly influence the outcome despite efforts to maintain neutral and objective (Hirsjärvi & Hurme, 2017). For adding to the dependability, an iterative approach was applied to the data analysis to ensure consistency and transparency. Additionally, as mentioned previously, the guidelines for thematic analysis by Braun and Clarke (2022), and the instructions for content analysis by Tuomi and Sarajärvi (2002/2018) were followed similarly regarding the analysis of each participant's data. Lastly, these established guidelines for data analysis were also used because they have been previously proven to be dependable methods.

Fourth of the dimensions for trustworthiness, confirmability, was especially tried to improve by using method triangulation. Triangulation has been suggested by Hirsjärvi and Hurme (2017) to add to the confirmability of the results. In triangulation, data from multiple sources can be compared with each other, confirming findings (Hirsjärvi & Hurme, 2017). Although the data in this study was analyzed as a unified dataset, the findings still reflect insights from each triangulated method used, adding to the comprehensiveness of the findings. Additionally, most findings of this study align with previous research, which, as pointed out by Eskola and Suoranta (2014), supports confirmability. To further add to the confirmability, the previous research used in this study was carefully selected by paying attention to the rating of the papers and journals selected, as well as making sure that they were peer-reviewed. This ensured that the study had a solid base to build upon. Lastly, the data was revisited multiple times to verify themes and to ensure a consistent interpretation of the data, as recommended by Braun and Clarke (2022).

The methodological limitations of this study are related to the sample size and selection, potential research bias, and scope constraints. First, it is acknowledged that the findings are not generalizable beyond the sample group and demographic, as mentioned previously. Second, the participant's responses might be influenced by the research setting and the topic of discussion. For example, the participant might give answers that are more socially acceptable rather than authentic in the situation, and they might see the interviewer as intimidating and thus want to answer more generically (Hirsjärvi et al., 1997; Hirsjärvi & Hurme, 2017). While this was not explicitly observed during this study, all participants appeared genuine and honest in their responses. Additionally, interviews typically last for a long time, as they did in this study as well, and therefore the situation might get too friendly possibly leading to the interviewer losing their neutrality (Hirsjärvi & Hurme, 2017). These effects on the research bias were attempted to be limited by creating a neutral environment for the participants and the interviewer staying objective throughout the study, as suggested by Hirsjärvi and Hurme (2017). Furthermore, it was acknowledged that the findings of the study are at the end based on the researcher's own interpretations, posing a risk for subjectivity, despite the efforts to remain objective and neutral. Lastly, the time constraints for the master's thesis limited the depth of data collection and analysis, potentially affecting the findings' comprehensiveness.

5.6 Use of artificial intelligence in this thesis

In the writing process of this thesis, Generative Artificial Intelligence (AI) tools were used as assistants. More specifically, GPT-4 model by ChatGPT (Generative Pre-trained Transformer) (OpenAI, 2024a), SciSpace (2024), and Scholar GPT (OpenAI, 2024b) were used. All of these tools were used similarly, but the GPT-4 model seemed to function the best according to the preferences, and it was also the quickest of the tools mentioned. Therefore, the GPT-4 model was opted for most often. Additionally, Grammarly (Grammarly Inc., 2024) was used for reviewing the final thesis for any grammar mistakes and improving the academic tone. The use of AI tools in this study followed University of Jyväskylä's (n.d.) instructions and guidelines for using AI-based applications in studies.

Importantly, the use of AI tools did not compromise the originality of this thesis, as they were not used for directly generating content for it. Most importantly, the AI tools were not used in the data analysis process in any way or used for interpreting the results. Additionally, as forbidden in the AI tool guidelines by University of Jyväskylä (n.d.), AI tools did not assist with writing the abstracts in any way.

The AI tools were used, and found helpful, especially in refining the language and structuring the text. Language-wise, the tools were used to improve the academic tone of specific sentences that were sent to them - mainly giving better word suggestions. Additionally, language-wise, the tools were asked to present alternative ways of saying something and giving word suggestions for

describing something very specific. Content-wise, the AI tools were used to brainstorm ideas and organize them in a logical manner. Furthermore, the AI tools were found helpful in ideating comprehensive and brief titles to sections. Lastly, the tools were used to improve the cohesiveness and structure of specific pieces of text sent to them.

Any text or idea generated by an AI was critically reviewed and no output of it was taken for granted or as the absolute truth, as AI makes mistakes. As an exception to this, GPT-4 by OpenAI (2024a) was used to co-create practical examples for each deceptive pattern type in Table 1 in subsection 2.2.2 Types of deceptive patterns. The AI was sent the name and definition of the pattern and asked for a practical example of it in a cookie consent request.

6 RESULTS

In this chapter, the results of the empirical part of the study are presented. The chapter is divided into three sections. In the first section, the participants' perceptions of deceptive design's influence on their perceptions of privacy are presented in relation to each of the influencing factors from the theoretical framework. In the second section, other significant findings that influence the users' perceptions of privacy are presented. The third section focuses on users' impressions of deceptive design, cookies, and the cookie data collector.

6.1 Deceptive design's influence on users' privacy concerns, control over privacy, trust, and perceived privacy risks

The main goal of this thesis is to find how deceptive design influences the perception of privacy in cookie consent requests. This section presents the participants' perceptions of deceptive design's influence on each of the four influencing factors from the theoretical framework: privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks. Table 2 at the end of this section summarizes these findings, showcasing how the participants perceived their privacy regarding cookie consent requests without and with deceptive design.

6.1.1 Privacy concerns

A bit over half of the participants (5/8) found deceptive design to increase their privacy concerns. Many of them stated that deceptive design makes the cookie consent requests seem dishonest, unclear, and difficult to understand, which in turn was described as increasing their suspicion of the data collector's intentions, which further on increased perceived privacy risks as well. To illustrate dishonesty, unclarity and difficulty of understanding, participant P6 concluded these general thoughts of the participants in the following quotation:

Yup, the deceptive design does add [privacy concerns], because it makes me feel a bit uncertain... or like... I get the feeling that... when I see how badly they want me to accept everything, then it just makes me think that they are ready to use these kinds of dishonest methods to achieve it. [P6]

And the same participant P6 continues by saying that “It just makes me feel uncertain about what my information is actually used for. Because they are just so difficult to understand and trust.” The following statement encapsulates the core of the participants’ suspicions that were mentioned earlier:

Well I do get a suspicious feeling because like why... why do they want to do it like this... this button that I want to press, these settings, or something else... why does the website want to put it this way that it’s more difficult for me to find than the “accept all” button... so I just get that feeling that they somehow want to lure me to press that button by accident. Like what do they want this information for and why do they want it so bad? [P1]

Equally, participant P3 stated the same:

If they have to create the request in a deceptive way, then of course it makes me think what my data is actually used for at the end, and is it as safe as I think that it should be. So, yes, deceptive design does affect my control in a negative way. [P3]

However, the majority of these participants who thought that the privacy concerns were increased due to the use of deceptive design in the cookie consent request stated that the concerns were not increased considerably or enough to influence their perception of privacy negatively, just like participant P7 described it: “[Deceptive design] increases not only my degree of suspicion, but also my degree of worrying. But ultimately, not enough.”

The rest of the participants (3/8) did not see an increase in their privacy concerns due to deceptive design. The participants expressed to have so many concerns already related to their internet use and the collection of their personal information, that they did not find deceptive design to have enough influence to increase those concerns. Similarly, a few participants expressed that they did not want to think of the concerns because they felt enough in control of their privacy when using cookie consent requests and that deceptive design could not influence their perception of privacy. Not wanting to think about concerns was well articulated by participant P2:

I kind of try to keep my sanity by thinking that [sharing my cookie data] can’t be that bad, but then at the same time I kind of know the risks behind it... So, it’s a little bit of a confusion inside my mind, and then I just think if it would just be easier to like not think about these things [be concerned] and just use the web pages as usual. [P2]

The idea of control was brought up for instance, by participant P4 who said: “Deceptive design kind of doesn’t influence my concerns because there should always also be an option where I can edit my consent choice, so I usually look through the request carefully enough... so that I affect my choice.” Also, as an

example, one participant [P1] mentioned that deceptive design only increases their awareness of privacy and therefore they realize better the need for being in control:

I do have the feeling that a lot my information is being collected all the time and I don't have the energy to block that. So then, the concerns that I have of my privacy do remind me that I should remember that my information is being collected all the time... and then I just think that, oh, I should at least do the bare minimum that I can to protect my privacy, which is... to click decline or no thank you or something like that. [P1]

To summarize participants' general thoughts on privacy concerns, one participant put it as follows:

At the end, [deceptive design] doesn't influence enough because somehow I just think that I anyways need to use these services whether I trusted them or not, and then... I just don't have the energy to be concerned about them... so, at the end, it doesn't affect my concerns very much. [P6]

When participants described their privacy concerns regarding cookie consent requests that did not have deceptive patterns, most participants (7/8) expressed either not being concerned at all or only a little bit concerned because cookie consent requests are so common and normal part of their life, a ubiquitous experience, that they do not even think about their effects on them. This key observation was made by several participants, such as P2 and P6:

Yeah, yes [I am concerned], not too much but since the [cookie consent requests] are kind of everywhere, every time I go to a new website, they appear. So, then I kind of get numb to seeing them. [P2]

At the end not too much [concerns] because in some way I just kind of think that "Oh well, these services are almost mandatory to use no matter if I trust them or not." [P6]

To summarize, most of the participants saw an increase in their privacy concerns when deceptive design was used in a cookie consent request, but they did not think that deceptive design increases their privacy concerns enough to make their perception of privacy more negative. Some participants, on the other hand, did not see any connection between deceptive design and privacy concerns because they felt that they were already concerned about their privacy without deceptive design having been used. When deceptive design was not used in the cookie consent requests, most participants expressed little to no privacy concerns due to the requests' ubiquity. Lastly, it should be mentioned that no participant mentioned that deceptive design would have decreased their privacy concerns.

6.1.2 Control over privacy

Nearly all participants (7/8) felt that deceptive design either decreased their ability to control their privacy or made being in control more difficult. Multiple participants mentioned that control has a substantial influence on their privacy, but

what is interesting is that they did not think that deceptive design could influence their possibilities to control their privacy. The participants thought that being in control might become more difficult with deceptive patterns (such as, comparison prevention or misdirection) but despite that, the participants felt in control of their own privacy. This observation was made by several participants, such as participant P5: “If I have such a feeling that I can control the things related to my privacy, then yes, I have a perception that my privacy is in a better state,” as well as participant P4: “My experience is that no matter the design, the option for declining the cookies is always there somewhere and I can always find it and in that way control my privacy, even if they try to hide it with a deceptive pattern.” On the other hand, some of the other participants who felt that deceptive design clearly decreases their control described the influence of deceptive design as extreme, since they felt that their control was decreased so much that it made them frustrated and even anxious. To take it to the extreme, one participant [P8] described a general perception of deceptive design’s influence on control as non-voluntariness: “I can only see here an ‘accept all’ button, so it immediately makes me feel that I don’t have any other option than to accept all.”

In contrast to others, one participant [P7] had a different perception, as the following statement shows:

No, [deceptive design] doesn’t affect my control. As [cookie consent requests] appear in all the websites, I have the feeling that I am so used to them that I do not get fooled or my choice doesn’t get triggered by [deceptive design] directly. [P7]

Although, the same participant [P7] later stated that deceptive design might in fact make controlling a little bit more difficult:

The problem is that if the deceptive pattern really hides a button or makes finding it more complicated, then yes, of course... it in some way can affect my control indirectly. But I guess it depends on what deceptive patterns we are talking about. [P7]

The latter part of this statement is similar to many other participants’ [such as P5, P6, and P3] expression of control being design-specific – some deceptive patterns make it more difficult to control than others.

When the participants were asked about cookie consent requests that did not have deceptive patterns, two thirds of the participants (6/8) expressed to have full or partial control of their privacy, as participant P4 described it: “Well I do, I do feel that I have there the, like, a choice, and I feel that I have control when I can choose [the types of cookies that I want to be collected].” This aligns with another participant’s [P7] idea, saying:

I think I’m in control of, usually, let’s say an 80%, most websites let me be in control and usually even though that [the request] might be annoying, as I said, I know how to be in control or it’s clear how to be in control. [P7]

A significant finding is that control appeared to be, alongside with trust, the biggest and most remarkable factor influencing the perception of privacy, according

to the participants' responses. The participants often talked about privacy as control, even if the topic was not related to control. For example, the current interview theme might have been privacy risks but the participant often turned the discussion toward control.

To summarize, deceptive design decreased most of the participants' control over privacy. Contrary to this, when deceptive design was not used in cookie consent requests, most participants perceived to have either full or partial control over their privacy. As a final note, it should be mentioned that no participant expressed deceptive design to increase their perception of control.

6.1.3 Trust in the cookie data collector

Only one participant [P4] stated that deceptive design does not affect their trust in the cookie data collector. They validated this argument by saying: "I, like, want to trust [the data collectors] because it's also for their own benefit to be truthful and trustworthy" [P4]. The rest of the participants (7/8) stated that they had less trust in the cookie data collector when deceptive design was used. The participants described a few things to lower their trust: deceptive design makes it seem suspicious what the cookie data is used for, and deceptive design makes the cookie data collector seem dishonest. Dishonesty was well captured by participant P6: "If they use deceptive design, and they are not capable of doing it in an honest way, it doesn't inspire trust in me."

The participants also mentioned that using deceptive design in the cookie consent request makes it seem like the cookie data collector is not thinking what is best for the user, which in turn weakened their trust in the collector. To illustrate this, one participant [P3] said: "[The cookie data collectors], for sure, do not think what is the best for the user, they just think what is the best for them." Similarly, participant P6 stated: "It seems that [the cookie data collectors] are desperate to gather as much data as possible from me. So that makes me feel like the data is not gathered for my benefit, but instead for their own benefit and purpose." As a continuation, participant P8 described the collector to have a lack of professionalism due to the use of deceptive design, influencing their trust negatively. That made it seem that the collector's only goal was to gather user data with any available method possible.

The influence of deceptive design on trust was described with words, such as "diminishes", "breaks", and "shakes", such as the following quotation shows:

Yeah, it does shake my trust every time I see that they might be using a deceptive tactic. To start with, I usually have around 80-90% trust in the collector that they do everything okay and good, because we are all good people in our core, but the more I encounter a collector using deceptive design, even if they only use it a little bit, my trust just starts crumbling down and diminishing. [P1]

Some participants even stated to have no trust left toward the collector when they had seen that they use deceptive design.

The participants were asked about the cookie data collector's ability, benevolence, and integrity, as they were defined as attributes of trust by Mayer et al., (1995), as well predictability, defined by Gefen and Straub (2004). Approximately 6/8 participants did not find the cookie data collector to be competent, benevolent, or honest, when using deceptive design. Additionally, only some of the participants found the collector to be predictable in the context of deceptive design. These findings suggest that a cookie data collector who uses deceptive design is not seen as very trustworthy by most participants.

Contrary to distrust, when participants were asked about their trust in a cookie data collector who does not use deceptive design, the answers showed that the majority of the participants (6/8) trusted them. The following quotation by P3 encapsulates this idea: "Well I kind of do continuously trust them by accepting [cookie data collection] and thinking that my information does not end up in the wrong hands." Behind the remaining two participants' idea of not trusting a cookie data collector that does not use deceptive design was mainly the feeling of uncertainty about where their data is going to and how it is going to be used. Summarizing the general feeling of uncertainty, participant P4 stated: "Maybe in that sense I don't trust them because I can't, like, because I don't know where my information is going to. So therefore, I am a little bit cautious."

An important supportive finding from the data is that the participants often felt empathy toward the cookie data collector. The participants expressed that they would have wanted to trust the collector more because they wanted to think that maybe the collector is not using deceptive design on purpose or doesn't consciously want to cause harm to the user with it. To exemplify this, one participant said: "I don't want to think bad about them right away because they are 'just doing their job'. They might not be [using deceptive design] on purpose" [P8].

Alongside with control over privacy, trust was perceived to be the biggest and most remarkable factor influencing the perception of privacy, according to the participants' responses. The participants often talked about privacy as trust, even if the theme of the interview was not related to trust. For example, the interview theme might have been privacy risks, and the participant often turned the discussion toward trust.

To summarize, all but one participant perceived deceptive design to decrease their trust in the cookie data collector. Contrary to this, a cookie data collector who does not use deceptive design was seen as trustworthy by most participants. Interestingly, when deceptive design was used, some participants expressed empathy toward the cookie data collector.

6.1.4 Perceived privacy risks

Half of the participants (4/8) thought that deceptive design increases their perceived privacy risks. They expressed that deceptive design causes them to be uncertain and unsure about what their information is used for and who the information is shared with. As one participant [P5] put it: "Yeah, deceptive design does increase the feeling of risks being involved... Maybe that... I am like not sure what the information is being used for or that my information might be used

wrongly.” Conclusively these four participants thought that the biggest risk that deceptive design could cause is the misuse or illegal use of cookie data and personal information by the data collector or their partner. Interestingly, as an even more common response, the participants addressed their concerns about a risk of accidentally or unconsciously sharing too much cookie data due to deceptive design. The following response illustrates this fear:

Well, the risk that I see is the fact that because there are deceptive patterns in the cookie banner, I might click something that I don't wanna click and then my information may be shared with people that I don't wanna share... If the design is “incorrect,” I might be clicking something that I don't want to and therefore I might be in a bigger risk because I have shared more information that I intended. [P7]

The participants often expressed this fear of sharing too much information with the website because they directly thought that sharing unnecessary data will lead to less privacy. Similar to the findings about privacy concerns and trust, the suspiciousness caused by deceptive design increased the perceived privacy risks. One participant [P3] captured the core idea of this risk:

Well now that I think about it... so... if the request is not straightforward and tries to circle around any other option than accepting all cookies, like trying to bend the law... it kind of makes me think that there's something they are trying to hide that I don't understand or I don't know about... which in turn then makes me think that there are more risks involved in this website compared to some other website if I wanna share my cookie data with them. [P3]

Three participants stated that deceptive design had no influence on their perceived privacy risks and felt that there was no possible way that deceptive design could affect risks or the perception of them existing, as for example the following statement shows: “my idea of risks doesn't get triggered by how the cookie banner is designed, directly... I think they don't have direct relationship with the deceptive patterns” [P7].

Only one participant [P8] reported deceptive design to decrease their perceived privacy risks. When they were asked about this perception, they responded: “Because the deceptive design makes it clearer and easier to make the [accept all] choice, so I don't see there any risks in choosing wrong” [P8]. It was rare that a participant would have wanted to accept all cookies. Most of the participants mainly opted for the button for rejecting all cookies or adjusting settings.

Privacy calculus, as mentioned in the theoretical framework, can be used to define privacy risks' influence on the perception of privacy. Most participants (7/8) stated to often weigh the benefits with the perceived risks when deciding about giving their consent for collecting cookie data or entering the website after seeing the cookie consent request's design. But interestingly, none of the participants found deceptive patterns to help them or benefit them in any way. The participants normally weighed the benefits of visiting the website with the risks of consenting to cookie data collection. Two participants mentioned the deceptive patterns to potentially help those kind of people who want to accept all

cookies and share a lot of cookie data with the data collector, since deceptive patterns most often guides the user toward that option. 5/8 participants mentioned that deceptive design only exists for the cookie data collector's benefit, increasing the amount of data that they are able to collect and use for their benefit either inside their own organization or by selling the data to third parties and getting revenue from it. The following comments support this privacy calculus idea:

Probably it only benefits those people who are going to use the data from the website, but not the user, I think. I don't see there any benefits for me [with deceptive design]. I probably never even really think of [the benefits]. [P8]

So, [when deceptive design is used] it just feels like the information is not collected for my benefit, but for the collector's own benefit. [P6]

If they use deceptive design or something similar, then I might sometimes totally retreat, like then I won't even enter the website. Because then I kind of balance the idea of "will it be worth it to watch, for example, this video from this website if I don't actually need to watch it and I just want to watch it," so are then the risks of sharing my cookies bigger than the benefits I will get from watching the video. [P3]

When the participants were asked about cookie consent requests that do not use deceptive patterns, all participants' ideas of risks aligned: they knew that there are risks, and that it might be risky to share their cookie data, but they were not worried or concerned about those risks. The following statement encapsulates this idea: "I'm aware that there are risks, but... I don't have the feeling that I should be very worried about them" [P7]. One of the most common concerns related to the participants' perceived privacy risks about cookies in general (without taking deceptive design into account) was the fact that the users were unaware and uncertain about how or why their information is being collected and for what reasons, which in their words increases the probability of losing their privacy. This concern is transmitted, for example, through the following participant's comment: "So maybe I just think there to be a risk because you can never actually know what you are agreeing to or what [the cookies] are used for" [P8].

To summarize, participants' responses for deceptive design's influence on perceived privacy risks varied notably, reflecting three different perspectives. Out of eight participants, one found deceptive design to decrease their perceived privacy risks. On the contrary, four participants found deceptive design to increase their perceived privacy risks. The last three participants perceived deceptive design to have no influence on perceived privacy risks. Regarding the privacy calculus theory, the majority of the participants perceived there to be no benefits but only risks related to deceptive design. When deceptive design was not used in cookie consent requests, the participants still perceived there to be risks related to their privacy, but they were not concerned about it.

The following table 2 summarizes the findings of this section 6.1, showcasing how the participants perceived their privacy regarding cookie consent requests without and with deceptive design. The table separates the participants' perceptions of deceptive design's influence on each of the four influencing factors.

TABLE 2 Users' perceptions of privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks in cookie consent requests without and with deceptive design

COOKIE CONSENT REQUESTS WITHOUT DECEPTIVE DESIGN	COOKIE CONSENT REQUESTS WITH DECEPTIVE DESIGN
Privacy concerns	
*7/8 participants were only slightly or not at all concerned about privacy	*5/8 participants found deceptive design to increase their privacy concerns, but they did not think that it is increased so much that it would influence their perception of privacy negatively *3/8 participants did not see an increase in their privacy concerns, since they thought that the concerns remained the same despite deceptive design
Control over privacy	
*6/8 participants felt they had partial or full control over their privacy	*7/8 participants felt that deceptive design decreases their control over privacy *1/8 participants felt there to be no connection between control and deceptive design
Trust in the cookie data collector	
*6/8 participants trusted the data collector *2/8 participants expressed mistrust	*7/8 participants stated that they had less trust in the cookie data collector if the request had deceptive design patterns *1/8 participants trusted the data collector who uses deceptive design
Perceived privacy risks	
*8/8 participants acknowledged potential privacy risks but were not concerned about them *Privacy calculus: some benefits in cookies	*4/8 participants stated that deceptive design increases risks *3/8 participants saw no connection between risks and deceptive design *1/8 participants saw a decrease in risks due to deceptive design *Privacy calculus: more risks than benefits in deceptive design

6.2 Additional findings influencing the perception of privacy

In this section, some other notable findings that influenced the participants' perceptions of privacy are presented, as they were significant regarding the research questions. Next, the following topics are presented: user's personal interest's influence; the importance of deceptive design compared to other influencing factors; deceptive design's influence on privacy attributes; design-specificity of perceptions; ubiquity of cookie consent requests and deceptive design; and lastly, avoidance of the topic.

6.2.1 User's personal interest

Most participants (6/8) commented that their personal interest toward their privacy and thus, their own active control over their privacy, is a more meaningful influencing factor for their perception of privacy than deceptive design or any of the other influencing factors from the theoretical framework. The following comments support this idea:

It makes me feel that this [cookie consent request] is like a game that I have to play, like I am kind of forced to be cautious of my privacy in them... I just think that "he is not dumb who asks, but the one who pays" [A Finnish saying, literal translation]. [P2]

I will say, though, that the control is quite a big part of my privacy... even just the fact that I know what my private information is used for when I have chosen only specific information to share has a big influence on how I perceive [the state of my privacy]. [P2]

Your privacy is like dependent on yourself only, like how carefully you wanna look through the [cookie] options. [P4]

I understand the idea of [deceptive patterns] trying to make you look somewhere, but you just have to be aware and smarter than them and be very, like, eyes open and just not click on that. [P7]

Interestingly, some of the participants found it important and useful to be educated on the topic during the interviews. They, for example, stated that normally they would not have thought about their privacy but after learning about the topic and being more aware of it, they expressed a positive influence on how carefully they might behave online in the future regarding cookie consent requests. For example, they might be more cautious of the consent choice that they make and be more aware of deceptive patterns guiding them.

6.2.2 Importance of deceptive design's influence in comparison to other factors

Diminishing the influence of deceptive design on the perception of privacy, some participants (3/8) stated that the perception of privacy is not solely dependent on deceptive design, but rather it is a combination of multiple influencing factors, as participant P5 put it: "Well yeah, [deceptive design] can have an effect on privacy, but at the end my perception of privacy is a combination many things." Contrarily, 5/8 participants emphasized that compared to the other influencing factors (privacy concerns, control over privacy, trust, and perceived privacy risks) deceptive design has a notably bigger, if not the biggest, influence on their perceptions of privacy. This idea was backed up mainly by the fact that deceptive design is the first and most noticeable thing that the user sees when encountering a cookie consent request. The following statements support this finding:

Probably the deceptive design patterns have quite a big influence on my perception [of privacy] because it's maybe even the easiest thing to notice. Like I can't even notice the other things that might be happening in the background, like the risks for example, so yeah, I think [deceptive design] is quite an impactful factor. [P6]

I think [deceptive design] has the biggest role because the first thing that catches your eye on the website is the cookie banner: the colors, the form, the size of a banner, the size of the letters that are actually important, the text that is very small... So, that's the first thing that you see. And even though that the perception [of privacy] might be built by many small things, the deceptive pattern is really the first impression, let's say it like that. [P7]

In many cases yes, deceptive design influences my [perception of] privacy the most... because the cookie request is the first thing that appears that I see. [P1]

6.2.3 Privacy attributes and design-specificity

The participants were given a list of fourteen privacy attributes by Barth et al. (2022) during the interviews, as introduced in section 3.2 Privacy-protective design. The participants expressed that deceptive design influences their perception of each of these attributes negatively in some way, but the attribute that was the most notably influenced was transparency. The participants perceived that due to deceptive design, the transparency was either reduced or even totally missing from the cookie consent request when it involved deceptive patterns, as it is exemplified in the following citation during which the participant was attempting to make a choice between accepting all cookies and “No thank you, I want a bad user experience”:

So, I can't immediately find the information about what my cookie consent and data would be used for... I can't find the actual facts about it. And maybe there could be something else going on that is not told. Like, is there something else included in this [accept all option] that I would be interested in knowing as a user? [P2]

The participants expressed the four following attributes as the most important to be taken into account in a cookie consent request to improve their perception of privacy: purpose, security, transparency, and anonymization. Of these, purpose - the clear explanation for why personal data is being collected - was ranked as the most critical, followed by security - the informed protection measures to safeguard users' cookie data. Transparency regarding the organization's data practices was also highly valued, as it increased trust. Additionally, anonymization - editing personal data so that it cannot be directly traced back to an individual - was perceived as a meaningful factor in enhancing the perception of privacy.

Lastly, half of the participants (4/8) emphasized in their answers that their perceptions are always design- and context-specific. Even when it came to deceptive design, they stated that their perceptions varied depending on the type of deceptive pattern that was used. This idea is exemplified in the following statement: “Well, I think [my privacy perception] varies a lot. There are so many

different [designs]" [P4]. This finding was especially related to the topic of control over privacy but it was also mentioned elsewhere in the interviews.

6.2.4 Ubiquity and avoidance of the topic

Many participants (5/8) perceived deceptive design to be a common part of their internet use. The participants described being used to avoiding the consent choice options that deceptive patterns try to guide them toward, for example, by directly looking for the option that is not highlighted, expecting it to be "decline all" or "settings". To illustrate this, participant P1 said: "'Save settings' is again the smaller option but I'm already used to that." Another participant also stated that: "Even though that this [accept all button] is green and it's more eye catching again, but I am very used to that eye catching thing, so I would just click here [gray button: decline]" [P7]. Some participants even stated that due to deceptive design's ubiquity they have learned to be more careful when selecting their consent choice. This is exemplified in the following comment:

Normally I... or like... these days I feel like I'm like used to it... I have learned that I will look carefully through [the consent options], like what does the most tempting button say, for example, because if that has been made easy then you can directly see from the button if it is what I was looking for that I wanted to select. [P1]

5 out of 8 participants noted that it was difficult to describe how they feel about their privacy regarding cookie consent requests since they have become such an ubiquitous part of their daily internet use and that they barely even notice the cookie consent requests or sharing their personal data when browsing the web. For instance, participant P6 mentioned: "I actually don't even think about that ever because [using cookie consent requests] has become such an automatic task that I do not even think about anything while doing it." Similarly, participant P3 stated: "In a way [a cookie consent request] is such an everyday thing, and therefore I have not even stopped to think about it." The same participant [P3] also said that they had not even realized how often the requests occur and that their privacy is also tied to using cookie consent requests because the requests are such a "regular occurrence" that one might think that there is not even a need to think about their privacy.

At times, some participants (3/8) additionally expressed their own privacy to be a difficult and sometimes even a scary topic. This translated to them avoiding thinking about it in their daily lives. One participant even described it as follows:

It feels like I'm standing on the edge of an abyss [a saying conveying a sense of being near something deep, dark, and unknown, with fear and uncertainty about the topic], so would it then just be easier to not think about it and just continue using the service as usual? [P2]

6.3 Users' impressions of deceptive design and cookies

In this section, users' impressions of deceptive design, cookies, cookie consent requests, and cookie data collectors are presented. The section is divided into three subsections: emotions and cognitive states, descriptions of deceptive design in cookie consent requests, and descriptions cookie data collectors. In each subsection, commonly occurred emotions, cognitive states or descriptive words related to these topics are introduced.

6.3.1 Emotions and cognitive states regarding deceptive design in cookie consent requests

It was clear that deceptive design awakened only negative emotions and cognitive states in the participants. The participants expressed annoyance and even anger (expressed by 7/8 participants) toward the use of deceptive design in cookie consent requests, as the following statement shows:

Well, it makes me angry. It like frustrates me because I just wanna be able to complete [the request] as effortlessly as possible. And when it's not effortless and easy then it just like annoys me because it takes my time from something else. [P4]

The deceptive design was also perceived to create some uncertainty and unawareness (expressed by 6/8 participants) of what the users' information was used for and who it was shared with, since deceptive design made it more difficult to understand and find information related to those questions. These cognitive states are encapsulated in the following quotations:

It's often unclear what all my information is actually used for. And also, like, do I trust then that the information is used for only what I give permission for. So maybe it's just that they are so difficult to understand and trust in the first place. [P6]

It's not very well clarified here how my own experience would change if I chose [to consent to] one or the other. So, I can't easily find it right away what the information would be used for... I feel like [declining the consent] because I'm not getting enough information. [P2]

The participants' general negativity toward deceptive design was also a common theme in the interviews (clearly expressed by 5/8 participants). To exemplify this, participant P7 stated deceptive patterns to be "totally negative all the time." The data included no positive emotions or cognitive states related to deceptive design.

Similarly, participants expressed negatively associated emotions regarding cookie consent requests in general, without paying special attention to deceptive design. Multiple participants stated cookie consent requests to be something annoying even if they had found them to be useful or positive, such as P7 said: "I mean it's very annoying, but I understand the cookies ultimately as something

positive for me.” Equally, cookie consent requests were found to bring anxiety to the users, as exemplified by one participant’s comment:

Like do I have to every single time while browsing the internet activate my mind for making a decision [about my cookie preferences] because that might bring me a bit of anxiety and stress when I realize that I can’t just browse the web without thinking about anything and instead have to be quite cautious about what I click on and what I give permission to. [P2]

Some signs of frustration were as well seen in the participants’ answers regarding cookie consent requests in general - when deceptive design was not included - as for example, participant P1 stated: “Damn it, they always appear and block my visit to the website, I wish I could just browse the web in peace.” Some participants even described cookie consent requests to be a block to their end goal (accomplishing a task on the website or accessing the website). For example, participant P1 said: “You just always have to consent to something so that [the cookie consent request] goes out of the way so that you can use the website,” while another participant [P4] noted: “Well, maybe [the request] just slows down the visit.”

Contrary to the participants’ negative emotions about deceptive design, cookie consent requests without them were mainly seen as something positive. If a participant perceived cookies as useful in their life, they also stated cookies to be something positive rather than negative to them, as it was highlighted by participant P7: “All the time I have the feeling that the cookies are more positive than negative.”

6.3.2 Descriptions of deceptive design in cookie consent requests

The participants described the use of deceptive design mainly with negative words such as suspicious (expressed by 6/8 participants), as it was already mentioned regarding deceptive design’s influence on users’ privacy concerns. The participants expressed this view in the following examples:

So, the first thing that comes to mind is that it is a red flag [= a warning sign] that the “No thank you, I want a bad user experience” option is super small here at the bottom. And I start feeling like “Umh, okay, what’s the deal with this being this way?” And the alarm bells start to ring in my head like “Okay, so they are trying to guide me now,” and then I have to start being very careful with what I consent to. [P2]

Yeah, I start suspecting [the cookie consent request]. Why is it that they really, really, really want me to accept all the cookies? [P7]

The deceptive design patterns seemed to make the requests unclear and uninformative or even unpredictable (expressed by 5/8 participants) in the sense that the participants did not know where their information was going to and what it was used for, since deceptive design made it difficult to understand the requests (as mentioned by 5/8 participants). A few participants (3/8) stated that deceptive patterns made the requests complicated since it was often difficult to find an

option to decline consent or edit settings. These impressions emerge in the following examples:

It's a lot of work to like figure [the cookie consent request] out... Like sometimes it's designed in a very difficult way, the interface might look like a piece of code to me [a non-programmer] and then I have to read through it very carefully because it doesn't appear to be simple at first glance. [P2]

Usually if [the design is] deceptive then the information is also harder to find. [P4]

Deceptive design makes me think that [the cookie data collectors] do not want to provide understandable information. [P8]

[Deceptive design] makes it more difficult to get the information or like somehow distorts it... or it makes it more difficult to make the choice that I want, so yes, [deceptive design] does affect by making it more difficult. [P6]

The deceptive design patterns were described as persuasive by 3/8 participants, and even as manipulative by two other participants. The request being persuasive and complicated made it seem to most participants (5/8) that it was not voluntary to make a choice other than accepting all cookies. The following quotations highlight these shared experiences:

[Deceptive patterns] try to persuade or guide me toward accepting all of these cookies... so it guides quite a lot toward [accepting] then. The option for accepting looks much more tempting to click on but despite it will click "I want a bad user experience." [P5]

[Deceptive design] kind of is, dare I say, conscious manipulation of the user. [P3]

[Deceptive design] gives me the impression that I don't have that choice [to decline]. [P4]

The data did not reveal any evident positive descriptions of deceptive design.

As opposed to the way that deceptive design was described by the participants, cookie consent requests in general were seen as easy to use and understand. This opinion can be seen in the following quotation: "Yeah, I think making the choices is very easy. It's very easy. I think I understand everything" [P7]. But of course, the usability and simplicity always depend on the design of that particular cookie consent request, as participant P8 put it: "Depends on how they have designed it. Sometimes they are very scientific or like very hard to understand and then others are very simple. So, it depends." Similarly, at least half of the participants (4/8) found cookies to be useful and therefore something positive in their daily life. The useful features of cookies that were mentioned were mainly that the functionality of the website improved [mentioned by P1 and P3] and that the advertisements and content of the website were personalized to their interests [mentioned by P7, P3, and P8].

6.3.3 Descriptions of cookie data collectors

The participants liked to express how they felt about the cookie data collector. The most common themes that were found were non-benevolence (as described by 6/8 participants), dishonesty (as described by 4/8 participants) and incapability (as described by 4/8 participants). Participants expressed these views in the following examples:

[The cookie data collectors] are not always benevolent. Some of them probably only [use deceptive design] for money and do not think of my privacy at all in that situation. [P8]

[The cookie data collectors] are... and this is a mean way to put it... but I kind of feel like saying that they treat me in a degrading way. [P2]

If [the request] is designed deceptively then it immediately makes me question whether [the collectors] are honest and telling me everything. [P1]

[Deceptive design] projects a certain lack of professionalism. Like it doesn't feel at all like [the request] was designed by a professional. [P8]

Although, as mentioned previously in subsection 6.1.3 Trust in the cookie data collector, many participants felt empathy toward the collectors and did not necessarily want to think bad about them.

7 DISCUSSION

In this chapter, the key findings related to the research questions are presented and discussed in the light of previous research and theories. Additionally, contributions for both theory and practice are presented. Lastly, the limitations of the study are considered, and future research ideas are suggested.

The study aimed to investigate how users perceive their privacy when encountering cookie consent requests that are designed with deceptive patterns. A closer look was taken to uncover deceptive design's influence on the users' perceptions of privacy. The research questions were explored using data collected during the empirical phase that was conducted with method triangulation: combining user testing with a think-aloud method, supported by thematic interviews. The following questions were analyzed within the context of the theoretical framework and other supporting theories, using content and thematic analysis:

Q1 How does deceptive design influence users' perceptions of privacy in cookie consent requests?

Q2 What are users' overall perceptions of privacy in cookie consent requests that include deceptive patterns?

Both research questions focus on users' perceived sense of privacy, rather than measuring their behavior or deceptive design's actual effects on privacy or security. The following two sections present the answers to each of these research questions individually and interpret them in the light of existing literature and theories.

7.1 Deceptive design's influence on users' perceptions of privacy in cookie consent requests

This section covers the key findings related to deceptive design's influence on users' perceptions of privacy in cookie consent requests. The findings are

presented and discussed following the theoretical framework for the perception of privacy and its four influencing factors: privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks. Followed by other key findings regarding deceptive design's influence. Finally, concluding with deceptive design's overall influence on the users' perceptions of privacy.

Deceptive design's influence is examined both regarding each influencing factor, as well as its conclusive, overall influence on the perception of privacy. Users' impressions of deceptive design, cookie consent requests, and cookie data collectors play an important role in shaping these findings.

7.1.1 Influence on users' privacy concerns

The most prominent finding regarding users' privacy concerns was that the users experienced an increase in their privacy concerns when deceptive design was used in cookie consent requests. Aligning with this finding, Mathur et al. (2021) have found that users generally have privacy concerns when deceptive design is used. The results of the current study show that the increase of privacy concerns was caused by the participants perceiving the cookie consent requests as unclear, difficult to understand, and dishonest, when deceptive design was used. Supporting these impressions, previous research by Gray, Chen, Chivukula, and Qu (2021), Lupiáñez-Villanueva et al. (2022) and Maier and Harr (2020) have found similar descriptions related to deceptive design, although their studies were not conducted in the context of cookie consent requests.

Adding interest to the findings, some participants of the current study viewed deceptive design's influence on their privacy concerns as not substantial enough to noticeably change their overall perception of privacy, possibly because they were already concerned about their privacy without deceptive design having been used. This finding is similar to studies by Alharbi et al. (2023), Gray, Chen, Chivukula, and Qu (2021), and Ha et al. (2006) that found users to already have privacy concerns related to cookie consent requests even before deceptive design was introduced. The findings of the current study, supported by previous research, suggest that users' privacy concerns are not majorly influenced by deceptive design, as users already perceive cookie consent requests as concerning in the first place.

Another key finding is related to users' suspicions. A study by Mejtoft et al. (2023) found that users perceive the use of deceptive patterns as suspicious, which in the current study was seen as a factor that increased the users' privacy concerns in cookie consent requests. Related to the suspicions, the users in the current study expressed heightened uncertainty about what their data was being used for when deceptive design was included. Interestingly, a previous study by Singh et al. (2022) found that cookie consent requests in general, without including deceptive design, were also perceived as suspicious by users. These contradictory findings, as mentioned in the previous paragraph, suggest that there is not a remarkable difference in users' perceptions with or without deceptive design being included in the cookie consent requests.

Lastly, some of the users of this study were not at all concerned about their privacy when deceptive design was used in the cookie consent requests. Aligning with this finding, Bongard-Blanchy et al. (2021) have found that users generally are not concerned about their privacy when deceptive design is used. This finding, although being only perceived by a few participants in the current study, could further reduce the idea that deceptive design increases users' privacy concerns.

To conclude, deceptive design may cause privacy concerns in users. Interestingly, deceptive design does not necessarily lead the users to have heightened concerns when compared with cookie consent requests without deceptive design.

7.1.2 Influence on users' control over privacy

As a key finding of the current study, deceptive design considerably reduced the users' control over their privacy. It was found that most users perceived deceptive design to make it more difficult to control their privacy, leading some users to even experience negative emotions such as anxiety or frustration. This finding about the diminished control aligns with a study by Gray, Chen, Chivukula, and Qu (2021) in which users perceived deceptive patterns as difficult and complicated. Supporting deceptive design's negative influence on users' perceived control over privacy, the results of the current study showed that when deceptive design was not included, the cookie consent requests were found easy to use and understand. This finding suggests that users perceive to have more control over their privacy when deceptive design is not used in a cookie consent request.

However, previous research has shown that cookie consent requests without deceptive design also generally seem difficult to use and understand (Habib et al., 2019), as well as frustrating (e.g., Ha et al., 2006; Kulyk, Hilt, Gerber, & Volkamer, 2018; Mejtft et al., 2023; Nouwens et al., 2020). These findings contradict the findings of the current study, suggesting that the use of deceptive design makes no difference regarding users' perceptions of control in cookie consent requests. Although, it is worthy to mention that the previous studies mainly focused on perceived control in general, and not on control over privacy specifically.

Consistent with the study by Nouwens et al. (2020), the current study found that deceptive design makes the cookie consent choice non-voluntary, enhancing the users' perceptions of reduced control. Likewise, the current study found cookie consent requests that included deceptive design to be perceived as persuasive and manipulative, which aligns with the users in the studies by Gray, Chen, Chivukula, and Qu (2021) and Maier and Harr (2020) describing deceptive design itself as forcing, triggering, and aggressive.

To conclude, this study suggests that deceptive design causes a decrease in the users' perceptions of control over their privacy, supported by users' negative impressions of deceptive design and the users' idea of non-voluntary consent. However, the findings from previous research partially suggest that the perception of control might not be solely influenced by deceptive design, as similar perceptions of control have been found regarding cookie consent requests in general,

without deceptive design. Further examination would be of use to understand what a user's perception of control over privacy consists of, especially regarding design choices.

7.1.3 Influence on users' trust in the cookie data collector

The findings suggest that users' trust in the cookie data collector is compromised by deceptive design. This finding reflects the one by Lupiáñez-Villanueva et al. (2022) who also found that deceptive design leads to most users having less trust.

One reason for the diminished trust in the current study was the users' suspiciousness of what the cookie data is used for, such as it was also found by Mejtoft et al. (2023). Another suggestion is, as the current study's results show, that the users' perceived dishonesty of the cookie data collector diminishes trust. Supporting this finding, Maier and Harr (2020) have also captured users describing the organization as dishonest when they have used deceptive design - further weakening their trust. Contrary to these findings, a study by Keleher et al. (2022) found that users generally perceive deceptive design as something positive, ethical, and honest, arguing that experts might often incorrectly assume users' perceptions. Still, these findings by Keleher et al. (2022) are in the minority when looking back to the previous research introduced in subsection 2.2.4, and it may be taken that the current study's findings of distrust and dishonesty are genuine perceptions of users as they align with most of the previous research.

An additional reason for mistrust in the current study was the non-benevolent nature of the cookie data collector, according to users' perceptions. This finding was similarly found in a study by Gray, Chen, Chivukula, and Qu (2021) - users perceived that the organization is only thinking of their own benefit, undervaluing the users. Since Mayer et al. (1995) have argued that the benevolence of the trustee is one of the key building blocks of trust, it may be taken that the non-benevolence found in the current study further indicates deceptive design's negative influence on trust.

Providing further support for deceptive design causing mistrust in users, the current study found that some users even perceived there to be no trust left toward the cookie data collector when deceptive design had been used. Furthermore, giving additional support to the idea that deceptive design causes mistrust, the users in the current study appeared to trust the cookie data collector more when deceptive design was not used.

Interestingly, similar to a finding about users' sympathy by Gray, Chen, Chivukula, and Qu (2021) and Lupiáñez-Villanueva et al. (2022), it was found that some users in the current study felt empathy toward the cookie data collector and wanted to trust them more. Still, this finding cannot considerably counter-balance the overall lack of trust that deceptive design appears to cause for the users in this and previous studies.

To conclude, the findings of this study, combined with previous research, indicate that deceptive design is directly linked to diminished trust. This mirrors previous studies (e.g., Lupiáñez-Villanueva et al., 2022) defining transparency - which is contrary to deceptive design - as increasing users' trust.

7.1.4 Influence on users' perceived privacy risks

The findings related to deceptive design's influence on users' perceived privacy risks were less conclusive, with users' perceptions varying. The results show a division in users' perceptions on the influence, with half of the users perceiving heightened privacy risks, and less than half reporting no influence. Interestingly, one user even perceived deceptive design to reduce privacy risks. Due to the varying findings in the current study, there is no clear consensus on whether deceptive design distinctly influences perceived privacy risks. Previous research shows similar variance in findings. In multiple previous studies (e.g., Bongard-Blanchy et al., 2021; Gray, Chen, Chivukula, & Qu, 2021; Mathur et al., 2021) it has been found that users perceive there to be risks related to deceptive design, but as Ha et al. (2006), Beckwith (2003), and Flinn and Lumsden (2005) have found, the users often do not find these risks threatening or affecting their behavior.

It has been suggested that users find it difficult to evaluate privacy issues, such as privacy risks, as they are not adequately educated on the topic (Beckwith, 2003; Flinn & Lumsden, 2005). This finding is similar to the one by Keleher et al. (2022) who stated that users could have different perceptions of deceptive design if they were better educated on the topic. The findings of the current study, on the other hand, do not directly support the idea of education or knowledge on the topic causing the users to view it any differently, since the participants were made aware of what cookies, cookie consent requests and deceptive patterns are. The participants in the current study were as much aware of the topics as they could at that moment, and still, the findings of users' perceptions were largely negative, aligning with the findings from previous research for the most part. Of course, it would be important to better educate users on the topics of this study, but first education's actual impact on users' perceptions of privacy could be researched, since at this state it cannot be reliably proven that increased awareness would influence these perceptions.

Regarding cookie consent requests that do not include deceptive design, it was found that users perceive there to be privacy risks, but they are not concerned about them. This finding adds to the uncertainty of deceptive design's influence on perceived privacy risks, as the size or type of risks could not be definitively compared in the presence or absence of deceptive design in cookie consent requests.

However, in line with the privacy calculus theory, the users' collective view leaned toward perceiving more risks than benefits related to the use of deceptive design, contributing to a slightly more negative perception of privacy. In line with Maier and Harr's (2020) study, the current study found that users perceive deceptive design to only benefit the organization who uses it. Continuing the consistency with Maier and Harr's (2020) findings, the current study shows that despite perceiving more risks than benefits, users would still continue using the service, as the benefits of entering the website outweigh the risks of deceptive design being included in the cookie consent request. Although here it is worthy to think again, whether having more knowledge on the topic would have an impact on the perceived privacy risks and thus the privacy calculus aspect as well.

To conclude, deceptive design's influence on users' perceived privacy risks was found to be subtle and inconclusive, with varying perceptions among users. This variability aligns with previous research, further questioning if users' awareness and education on the topic would influence perceived privacy risks. Lastly, despite perceiving more risks than benefits, users still preferred to take advantage of the website's benefits over the potential privacy risks related to deceptive design.

7.1.5 Other key findings regarding deceptive design's influence

Besides the previously presented findings of deceptive design's influence on the four influencing factors within the theoretical framework, there are other key findings that have an impact on deceptive design's overall influence on users' perceptions of privacy.

The current study found that users generally have negative impressions of cookie consent requests, both with and without deceptive design, as it has been similarly found by multiple scholars previously (e.g., Ha et al., 2006; Habib et al., 2019; Kulyk, Hilt, Gerber, & Volkamer, 2018; Mejtoft et al., 2023; Nouwens et al., 2020). Although, different from previous studies, the current study found users' impressions to become more negative when deceptive design is included in the cookie consent requests. This finding further supports deceptive design's negative influence on users' perceptions of privacy. Still, as users' impressions of cookie consent requests both with and without deceptive design have been largely similar, it may be suggested that deceptive design does not influence users' impressions as much as it may have been presumed solely based on the findings of this study on their own.

Interestingly, this study found that the ubiquity of cookie consent requests has led to a normalization of their use, diminishing users' overall concerns for their privacy. This finding about deceptive design's ubiquity was also reported by Di Geronimo et al. (2020), and Lupiáñez-Villanueva et al. (2022). In line with these findings, Mejtoft et al. (2021) found that users have started to experience something called "cookie blindness", which makes them function out of habit without seeing the content of the request more closely. This habitual exposure to deceptive patterns in cookie consent requests may influence how deceptive design is perceived, as users become conditioned to recognize and navigate deceptive patterns, possibly leading to desensitization regarding their privacy concerns. This habituation might also diminish the perceived emotional impact of cookie consent requests over time. However, participants in the current study still expressed feelings of annoyance and frustration, suggesting that even ubiquity or "cookie blindness" does not lessen the negative impressions tied to deceptive design.

Additionally, it was found that users' personal interest toward privacy and proactive control over it considerably influenced their perceptions of privacy, often more than deceptive design itself. This finding aligns with Maier and Harr (2020) who found that users perceived to be able to protect their privacy as long as the users themselves were using the service with caution. These findings

indicate that while deceptive design plays an important role, individual user agency may ultimately be a stronger influencing factor for the perception of privacy. Although, contrary to this finding, users in the current study stated deceptive design to have a big, if not the biggest, influence on their perception of privacy. The significance of each factor on the users' perceptions of privacy could be further tested with a quantitative study, to be certain of each factor's actual influence.

The findings revealed that deceptive design negatively influences how well the specific privacy attributes (introduced by Barth et al., 2022), especially transparency, are perceived by the user. Cavoukian (2010) and Barth et al. (2022) have stated that incorporating privacy-protective design frameworks in the design process could mitigate users' privacy concerns and improve the protection of personal data. However, the findings of the current study suggest that at least the transparency attribute has not been followed, as the use of deceptive design makes the cookie consent request seem non-transparent. No previous research has before investigated this connection between deceptive design and the privacy attributes, although, Lupiáñez-Villanueva et al. (2022) have found users to perceive the service or website as less transparent when deceptive design is used. On the contrary, there might not be a major difference in how users perceive the transparency regarding cookie consent requests when deceptive design is used, because a study by Singh et al. (2022) has showed that cookie consent requests – without deceptive design – are perceived to lack transparency to start with. The findings suggest that transparency should be taken into account better when designing cookie consent requests to improve users' perceptions of privacy.

Lastly, the finding about design-specificity of users' perceptions of privacy should be highlighted, meaning that the perception of privacy varies depending on the deceptive pattern type. This finding, in accordance with Lupiáñez-Villanueva et al. (2022), is a reminder that although the results show a predominantly negative influence of deceptive design on the users' perceptions of privacy, the findings are context- and design-specific and should not be generalized to all types of deceptive patterns and contexts.

7.1.6 Concluding remarks on deceptive design's influence on the perceptions of privacy

Conclusively, the key findings of this study indicate that users find deceptive design to negatively influence their perceived control over their privacy and their trust in the cookie data collector. Interestingly, the users also considered these two factors, control and trust, to be the biggest and most remarkable factors regarding their perception of privacy. However, deceptive design's influence on users' privacy concerns and perceived privacy risks was found to be more subtle, with varying perceptions on the factors. When compared to cookie consent requests without deceptive design, adding deceptive design to the requests leads to a clear shift toward more negative emotions and cognitive states, and ultimately, a more negative perception of privacy. Although this study cannot definitively establish deceptive design's overall influence on users' perceptions of

privacy, it can nonetheless be concluded that deceptive design generally tends to negatively influence users' perceptions of privacy.

This conclusive finding of deceptive design's negative influence on the perception of privacy is consistent with that of Graßl et al. (2021) and Mathur et al. (2021), although their studies did not use the same theoretical framework as the current study. Additionally, the conclusive findings of the current study align with Gray, Chen, Chivukula, and Qu (2021) who have reported deceptive patterns to cause users to perceive a lack of privacy.

Furthermore, while the influence of deceptive design on users' perceptions of privacy seems notable, and the users in this study state deceptive design to be the most visibly influencing factor for their perception of privacy, it was found that at the end, users' overall perception of privacy is influenced by a combination of various factors, reinforcing the idea that deceptive design is just one factor among multiple influences.

Lastly, it is important to question whether the findings of the influence of deceptive design on users' perceptions of privacy has any practical importance if the users' prevailing idea of cookie consent requests, as it was found in previous research, already is negative to start with. Would there truly be added value to the users, if deceptive design was removed from cookie consent requests? Maybe the root cause of negative perceptions of privacy is not deceptive design, but something else related to the context. One idea could be to figure out a totally new way of asking users' cookie consent in a way that does not cause any issues for users' privacy and does not conflict with users' goals of internet use.

7.2 Users' overall perceptions of privacy in cookie consent requests that include deceptive design

In this section, the findings regarding users' overall perceptions of privacy are presented in four subsections, somewhat aligning with the four influencing factors from the theoretical framework for the perception of privacy, combined with additional findings and users' general impressions related to deceptive design and cookie data collectors. Lastly, users' overall perceptions of privacy are concluded.

Regarding the key findings in this section, the data was analyzed in the light of users' subjective impressions or attitudes toward deceptive design and cookie consent requests. Rather than looking at deceptive design's influence on users' impressions, this section attempts to conclude whether users feel that their privacy is protected, respected, compromised, undervalued, or unimpacted when they encounter cookie consent requests that have deceptive patterns.

7.2.1 Perceptions of privacy: control

The results of this study point out a general loss of perceived control over the users' privacy, possibly caused by the feeling of being undervalued due to the

data collector's non-benevolence, and the feeling of being manipulated. This finding is supported by Gray, Chen, Chivukula, and Qu (2021), who found that users think that the collector is only thinking of their own benefit when using deceptive design. Similarly, cookie consent requests in general - without deceptive design - are in previous research found to be forcing and aggressive in the ways that they guide users toward certain consent choices (Maier & Harr, 2020). These perceptions of diminished control together contribute to a perception of users' privacy being undervalued or compromised when deceptive design is used.

Additionally, it was found that participants often wanted to consciously ignore the potential issues related to deceptive design despite being aware of their existence, as discussed later in subsection 7.2.3 Perceptions of privacy: privacy concerns and risks. Ignoring or minimizing the existing privacy issues could implicate that consciously interacting and constantly being aware - and thus, concerned - of the possible privacy issues would require more cognitive effort from the users than they would be willing to invest in their interaction with cookie consent requests.

7.2.2 Perceptions of privacy: trust and transparency issues

In this study, deceptive design seemed to diminish users' trust in the cookie data collector, mainly due to a lack of transparency and perceived dishonesty of the collector. These findings are consistent with previous research by Maier and Harr (2020), and Lupiáñez-Villanueva et al. (2022). Distrust and lack of transparency may be taken to indicate that the users perceive their privacy to be at risk because the findings contradict with the privacy-protective design principles introduced by Cavoukian (2010) and Barth et al. (2022). On the contrary, Keleher et al. (2022) found users to perceive deceptive design as more positive than negative - describing them as honest and ethical - suggesting that researchers often wrongly assume users' perceptions. In the light of the overall findings of previous research and the current research, the findings strongly indicate a more negative overall perception, contradicting the argument made by Keleher et al. (2022).

However, as similarly reported by Gray, Chen, Chivukula, and Qu (2021), some users expressed empathy ("sympathy" in Gray, Chen, Chivukula, & Qu, 2021) toward the cookie data collector, highlighting the complexity of users' perceptions: while they might not trust the data collector, they also recognize that not all of them consciously act maliciously. Despite the finding about empathy, the general lack of trust caused by deceptive design suggests an overall perception of the users' privacy not being well protected.

7.2.3 Perceptions of privacy: privacy concerns and risks

One finding in this study was related to the users' habitual engagement due to deceptive design and cookie consent requests' ubiquity and the users' general avoidance of thinking about the topic. Avoidance of the topic was found similarly in Maier & Harr's (2020) study, suggesting that users have a resigned attitude

toward privacy risks and issues due to deceptive design's prevalence in their daily life. This resigned attitude and habitual functioning of users might suggest that maintaining privacy is perceived as difficult, especially with the normalization of deceptive design. Likewise, the avoidance of the topic by some participants suggests an emotional complexity surrounding privacy. This finding indicates that fear or anxiety about privacy risks or issues may stop users from critically evaluating cookie consent requests, as similarly suggested by Lupiáñez-Villanueva et al. (2022).

Regarding the privacy calculus theory, it was found that although users often weighed the benefits with the perceived risks, they often ended up compromising their privacy for convenience. This finding suggests a more pragmatic view on privacy, as users often balance the convenience of quickly accepting cookies with the perceived risks of sharing their data. This pragmatic viewpoint aligns with existing research that has showed users to often function heuristically rather than rationally in consent-giving situations: functioning out of habit and making quick choices instead of rationally analyzing their choice (Graßl et al., 2021; and Utz et al., 2019). The heuristic behavior might explain why despite the users' awareness of privacy risks, they still end up accepting cookies without taking the privacy issues into account. These findings taken together suggest that users' perceptions of privacy might be unimpacted by the perceived privacy risks.

7.2.4 Perceptions of privacy: users' descriptions and reactions to deceptive design in cookie consent requests

In this study it was found that nearly all users had negative emotions such as frustration, annoyance, and uncertainty when encountering cookie consent requests that included deceptive patterns, leading them to doubt the cookie data collector's privacy measures and intentions. Similar negative emotions were found in previous research regarding deceptive patterns (see e.g., Bongard-Blanchy et al., 2021; Gray, Chen, Chivukula, & Qu 2021; Maier & Harr, 2020; Mathur et al., 2021). Although, compared with the previous studies, uncertainty was a unique feeling found in this study. But even uncertainty is similar to Machuletz and Böhme's (2020) finding about deceptive design making users regret their consent choices afterwards. The negative emotions, including uncertainty and regret might all stem from users describing deceptive design as complicated, unclear, and difficult to understand. These descriptions were also found in studies by Gray, Chen, Chivukula, and Qu (2021) and Lupiáñez-Villanueva et al. (2022). These negative descriptions and emotions suggest that users perceive a general threat to their privacy due to not being able to fully understand or be informed of the consequences of sharing their data.

Another finding of the current study is that deceptive design was commonly described as suspicious and misleading by the users, similar to the previous studies by Mejtøft et al. (2023), and Gray, Chen, Chivukula, and Qu (2021). These impressions reflect mistrust in cookie consent requests and cookie data collectors, as Mejtøft et al. (2023) also have suggested about deceptive design in general.

Additionally, the current study found users to describe the cookie data collectors as non-benevolent, dishonest, and even incapable. These descriptions of the cookie data collector have not been mentioned in previous studies, although, as argued by Mayer et al. (1995), benevolence and capability are crucial building blocks for trust, reducing the users' uncertainty about the trustee, and consequently improving their perception of privacy.

Conclusively, the prevalence of these negative descriptions might further indicate that the users' general perception is that their privacy - when deceptive design is used - is not being respected or protected as they would expect.

7.2.5 Conclusion on users' overall perceptions of privacy

Taken together, the findings suggest that privacy is not only perceived binarily as negative or positive, or protected or compromised, but rather the perception is a flexible concept that changes based on specific deceptive patterns and the users' own habitual behavior as well as interest toward protecting their privacy. This view is consistent with that of Lupiáñez-Villanueva et al. (2022) who argued that users' perceptions of deceptive design are always context- and design-dependent. Likewise, the current study showed that users perceive the different influencing factors of the perception of privacy (privacy concerns, control over privacy, trust, and perceived privacy risks) differently, and therefore the findings cannot be concluded into one general perception only.

However, the findings suggest that the overall perception of privacy in cookie consent requests with deceptive patterns, conclusively, is largely negative. The negativity stems from feelings of annoyance, frustration, mistrust, and uncertainty, combined with lack of control and the suspiciousness of the misleading and manipulative design choices. Although users may have learned to withstand or bypass deceptive design, the general perception is that deceptive design undermines and undervalues users' privacy, implicating a perception that the users' privacy is neither fully protected nor respected in cookie consent requests. These findings align with previous research by Gray, Chen, Chivukula, and Qu (2021) and Mathur et al. (2021), who have suggested that deceptive design undermines and diminishes users' privacy - although, no previous study has before concluded users' overall perceptions of privacy and has only focused on deceptive design's influence on specific individual factors or just users' general impressions on the topic.

Lastly, the theoretical framework created for this study is supported by the findings. The overall perception of privacy indeed consists of the four influencing factors that were mentioned, but additionally - for having a more comprehensive understanding of users' perceptions of privacy - the aspects of design and emotions could be included as separate factors in the theoretical framework.

7.3 Concluding summary of key findings

This section provides a brief summary of the key findings that directly address the research questions. The first research question: “How does deceptive design influence users’ perceptions of privacy in cookie consent requests?”, addressed the influence of deceptive design on users’ perceptions across four influencing factors: privacy concerns, control over privacy, trust in the data collector, and perceived privacy risks. The findings suggest that users find deceptive design to negatively influence their perceptions of control over their privacy and their trust in the cookie data collector. However, deceptive design’s influence on users’ privacy concerns and perceived privacy risks was found to be more subtle, with varying perceptions on the factors. Overall, deceptive design leads to a more negative perception of privacy compared to cookie consent requests without it, especially in terms of control and trust. Lastly, regarding the theoretical framework, there have been signs in previous research that design could have an impact on the perception of privacy. The focus of this study was deceptive design, and the findings support the idea of design being an influencing factor for the overall perception of privacy.

The second research question: “What are users’ overall perceptions of privacy in cookie consent requests that include deceptive patterns?”, explored users’ subjective impressions and attitudes toward their privacy. Taken together, the findings suggest that privacy is not only perceived binarily as negative or positive, or protected or compromised, but rather the perception is a flexible concept that changes based on specific deceptive patterns and the user’s own habitual behavior as well as interest toward protecting their privacy. Therefore, the findings cannot be concluded into one general perception only. However, the findings suggest that users tend to perceive their privacy as compromised, undervalued, and unprotected when deceptive design is included in cookie consent requests. The combination of mistrust, loss of control, and negative emotions related to deceptive design contributes to an overall impression that privacy is neither respected nor protected. Although users may have learned to withstand or bypass deceptive design, the general perception is that deceptive design undervalues users’ privacy.

Lastly, even though the study shows a predominantly negative influence of deceptive design on users’ perceptions of privacy, the findings are context- and design-specific and should not be generalized to all deceptive patterns and contexts. Still, the findings of this study, combined with findings from previous research and legislative measures, all suggest toward that deceptive design, in all its forms, should be avoided in the user interface of cookie consent requests.

7.4 Contributions to theory and practice

In this section, this study's contributions to theory and practice are represented. Starting the section with theoretical contributions and moving toward practical contributions.

7.4.1 Theoretical contributions

This study contributes to the growing literature on the perception of privacy by offering novel understanding on how deceptive design influences users' perceptions of privacy in cookie consent requests. Previous research has been largely quantitative, while this study focused on a qualitative, user experience-oriented standpoint to reveal a more in-depth look on users' perceptions, impressions, and attitudes on the topic.

While previous studies (such as, Adams, 1999; Chang et al., 2018; Dinev et al., 2013) have studied perceived privacy, this study attempted to make a difference between perceived privacy and the perception of privacy. It is suggested that the perception of privacy is not a binary or a static concept but rather it is a dynamic, and context- and design-specific, multifaceted topic. This study introduces a more flexible, subjective, and user experience-oriented dimension to the existing theoretical frameworks that have treated perceived privacy as a measurable, rational, and often static concept. Although, this study equally supports the previous models of perceived privacy when it comes to including the four influencing factors (privacy concerns, control over privacy, trust, and perceived privacy risks) in examining users' overall perceptions of privacy.

Regarding the theoretical framework and theories related to it, there have been signs in previous research that design could have an influence on the perception of privacy. One of the most important theoretical contributions of this study is the indication that design, specifically deceptive design, could be considered an influencing factor for the perception of privacy. The findings of this study show that not only does deceptive design influence the overall perception of privacy, but it also influences the four influencing factors individually. The findings related to impressions of deceptive design were largely supported by previous research as well.

Adams (1999) and Chang et al. (2018) have previously stated perceived privacy to mainly be an emotional response to the separate influencing factors, but they have not included emotions as a separate influencing factor in their research models. The results of the current study largely consisted of emotions and cognitive states, suggesting that adding them as separate factors to the theoretical framework of this study could be a valuable consideration in order to enhance the framework's comprehensiveness.

Unlike previous models and theories that focus primarily on rational reasoning of users' perceptions of privacy, this study suggests that by taking a user experience-oriented perspective and treating the concept flexibly, a more holistic understanding of users' perceptions could be achieved.

7.4.2 Practical contributions

This study has practical contributions for designers, developers, and policymakers, and ultimately, for end-users. The findings of this study highlight the importance of transparent, ethical and honest design in cookie consent requests. Deceptive design not only leads to a more negative perception of privacy and diminishes users' trust in the cookie data collector but also decreases the users' perceived control over their consent choice. As a result, designers and developers should take into account the privacy attributes that have been previously introduced by Barth et al. (2022) - paying special attention to the transparency of the design. Additionally, the current study suggests that practitioners should pay attention to design choices that enable user's own control when making a consent choice. These considerations align with the PbD principles by Cavoukian (2010) that advocate for privacy-protective default choices and user-centric design practices to promote trust and protect user data. The current study additionally found that cookie consent requests that incorporate deceptive patterns are perceived as undervaluing or undermining users' privacy. Therefore, practitioners should as well ensure that their cookie consent requests are informative about what data is collected of the users, what is the data used for and who is it shared with, as the study by Barth et al. (2022) has also suggested. Reflecting the findings of the current study, when the cookie consent request is transparent, clear, and user-friendly, it can create a more positive perception of privacy and additionally, build trust in the cookie data collector. To conclude, the findings of this study, combined with findings from previous research and legislative measures, all ultimately emphasize the need to discontinue using deceptive design in cookie consent requests' user interfaces to enhance users' privacy. Additionally, this and previous studies all support the adherence to the PbD principles by Cavoukian (2010) and the Privacy Attributes by Barth et al. (2022).

The findings of this study also suggest that policymakers should consider the impact of deceptive design on individual users' privacy when making new regulations. Existing cookie-related regulations could be strengthened to ensure that the requests adhere to privacy-protective design principles (by Barth et al., 2022; Cavoukian, 2010). Special attention should be paid to transparency and informed consent regarding the requests' design, so that the possibility of misleading users toward compromising their privacy - guiding them toward an option that is not optimal regarding their privacy - would be minimized. Privacy-protective design would not only help the end-users, but also possibly improve the organization's revenue if users perceive them as more trustworthy when deceptive design is avoided. Additionally, since the users in this study found deceptive design to degrade the usability and understandability of the request, adhering to the legislation and privacy-protective guidelines to avoid deceptive patterns would reduce the users' cognitive load regarding their internet use, improving their overall user experience.

This study also advocates for the adoption of design standards and guidelines. The findings of this study offer valuable insights of users' perceptions that could be taken into account in design standards or guidelines, which furthermore

could be adopted on a national or an organizational level. The findings indicate that the key influencing factors (privacy concerns, control over privacy, trust, and perceived privacy risks) could be integrated into the user interface design process, as the factors are integral for users' perceptions of privacy. Design standards that prohibit deceptive patterns could as well be more compliant with privacy regulations, such as the GDPR (2016/679). This study could be used alongside other existing literature to create and update privacy legislations and design standards. If privacy-protective principles, such as the ones by Cavoukian (2010) or Barth et al. (2022) are integrated into official standards, guidelines, or even regulations, it could not only improve users' privacy on an individual level but also make it easier for the organizations to meet regulatory requirements related to privacy on a practical level.

Lastly, this study, similar to Keleher et al. (2022), Utz et al. (2019), and Singh et al. (2022), supports the need for and importance of regulation to completely prohibit deceptive design practices and advocate for informed consent choices, as the use of deceptive design practices is not explicitly prohibited at the moment. The current study puts emphasis on regulating the use of deceptive design in consent-giving situations, which have an important role regarding users' ability to control the release of their personal data.

7.5 Limitations of the study

In this section, the limitations of the study are presented. The limitations relate to the sample size and the participants' demographic information, the participants' knowledge on the topics, typical limitations for qualitative research, and the designs of the mock-ups used in the user testing.

While the results provide valuable insights into the perceptions of the participants, due to the small sample size the results cannot be generalized into a larger user group. The participants also belonged to certain demographic groups: generation Z and university students. Likewise, the participants of this study were living in Finland, and could be subject to cultural or regional attitudes related to privacy, and their understanding of privacy laws could be different than that of people in other countries. Similarly, users' knowledge of the topics varied, possibly causing variation in their perceptions of privacy, despite the participants being shortly educated on the topic in the beginning of the interviews. Therefore, each participants' answers cannot be considered equal, as their knowledge was not examined as a factor in their overall perceptions. On the other hand, most of the participants did have different educational backgrounds when it came to the field of their studies, enriching the results.

The nature of the study was qualitative, and while it can provide rich and comprehensive findings, it can also reflect subjectivity (Hirsjärvi & Hurme, 2017). As participants' interpretations of the topic and their responses from emotions to perceptions can vary, the findings may not be replicable in a future study. Additionally, as suggested by Hirsjärvi et al. (1997) and Hirsjärvi and Hurme (2017)

the participants may not have reported their feelings or ideas accurately due to e.g., sensitivity of the topic, social desirability, or the strong emotions related to the topic. Similarly, the researcher's perceptions and presumptions may have had an influence on the way that the data was interpreted, as pointed out by Hirsjärvi and Hurme (2017), although a neutral perspective was attempted to take on.

The context of this study was cookie consent requests, and due to contextual differences the findings and contributions may not directly apply to other contexts such as privacy policies or terms of service, which despite being similar have other characteristics that would need to be taken into consideration.

Lastly, the mock-ups used in the user testing only included a specific set of deceptive patterns, which may not have accurately represented real-world designs. Although, this limitation was attempted to minimize by carefully selecting a variety of deceptive patterns to be included from previous studies' lists of most common deceptive patterns in cookie consent requests. Earlier in this study it was stated that participants' perceptions varied from design to design, which was also noted in previous research. Therefore, there is a possibility that the deceptive patterns chosen for the study's mock-ups were perceived differently than the ones that were not included in the study. Related to the same topic, the study did not comprehensively compare cookie consent requests with and without deceptive patterns in the user tests due to the limited resources for conducting the study. The results could have been more rewarding and extensive, if the cookie consent request mock-ups designed with deceptive patterns were compared with mock-ups that were designed following privacy-protective design guidelines.

7.6 Suggestions for future research

Although the study was attempted to conduct comprehensively and extensively, there still remains the need for further research due to this study's limitations and any ideas that arose from the findings of this study. The suggestions for future research are given in this section.

Although this study was able to qualitatively highlight the influence of deceptive design on users' perceptions of privacy, further quantitative research could be useful in understanding the specific significance of deceptive design's impact on the four influencing factors individually, to be able to understand which factors are the most sensitive to deceptive design's influence. Likewise, further research could attempt to understand which deceptive pattern types are the most harmful for users' perceptions of privacy. It would be especially interesting to know which characteristics of the deceptive pattern types influence the perceptions the most. Conducting these research ideas could additionally help in creating more specific privacy-protective design guidelines, when the most harmful aspects of design on users' privacy would be known.

Due to the study's limitations, the following factors' influence for the perceptions of privacy could not be investigated: the participants' demographic information, their knowledge and skills related to the topic, and their disposition

to value their own privacy. These were mentioned as possible additional influencing factors for perceived privacy in chapter 4, and they were already noticed to have some kind of influence on the participants' answers during this study's data analysis process. Although, they were not taken into account in the final results of the study. A quantitative study could better capture these factors' influences on the users' perceptions of privacy.

As the theoretical framework was not identical to prior research, and the findings that were detected using this framework were supported by previous research, it would be interesting to re-test the framework's transferability and thus trustworthiness in future research and add other dimensions to it as well, depending on the research context and aims. The framework could for example be tested in other privacy-related contexts, such as privacy policies. Optimistically, after testing the theoretical framework enough in different contexts, a conclusive qualitative research model for the perception of privacy could be shaped for others to benefit from in their research. An extended and further tested framework could also add to the understanding of how privacy experiences vary by design in different contexts.

During the interviews, the participants mentioned that they desired there to be an option to delete or edit their cookie consent choice after they had already given it. It would be interesting to study, how many or if any websites offer this option in the European Union or in Finland. It is a requirement in the GDPR (Regulation 2016/679) to have an option to delete the collected information and opt out from the consent afterwards.

When it comes to users' impressions of the data collector, this study only had a few findings related to it. It would be interesting to study more in depth how the users perceive the data collector when deceptive design is used. That type of research could possibly contribute to the research areas of marketing and brand image as well.

Since the participants' emotional responses and cognitive states were an important finding of this study, it would be interesting and useful to repeat this study with a specific emphasis on them. More specifically, the participants' emotional user experience could be studied regarding cookie consent requests that include deceptive design. To better implement this aspect in further research, specific research methods and analysis methods for studying emotional user experience should be investigated.

Lastly, due to the limitations of this study and the inability to generalize the findings to other contexts, a more comprehensive study on the same topic could be conducted to get more specific, generalizable results so that they could better contribute to, for example, expanding the privacy-protective design guidelines.

8 CONCLUSIONS

This study contributed to the increasing need to understand and protect users' privacy as deceptive design practices have become more prevalent (Di Geronimo et al., 2020; Lupiáñez-Villanueva et al., 2022), particularly within cookie consent requests, which play an important role in users' ability to control their own privacy (Alharbi et al., 2023). Despite privacy legislation - like the GDPR (Regulation 2016/679) - attempting to safeguard users' privacy, many organizations still use deceptive design in their services, undermining the intention of privacy legislation (see e.g., Alharbi et al., 2023).

To address this issue, the goal of this study was to find out how users perceive their privacy in cookie consent requests that include deceptive patterns, and what the role of deceptive design is in this perception. The study was conducted with method triangulation, combining user testing, the think-aloud method, and thematic interviews to comprehensively capture users' perceptions of privacy.

This study addresses a research gap by taking a qualitative, user experience-oriented perspective on the topic, and making a distinction between perceived privacy - a measurable, rational, and often static concept - and the perception of privacy - a fluid and subjective user experience. This study proposed a comprehensive theoretical framework for understanding users' perceptions of privacy through four influencing factors: privacy concerns, control over privacy, trust in the data collector, and perceived privacy risks, as inspired by previous models for perceived privacy (Adams, 1999; Dinev et al., 2013; Chang et al., 2018). Deceptive design's influence on users' perceptions was examined within this framework. The influencing factors were used as guiding themes throughout the study, not as measurable and absolute variables.

The findings reveal that deceptive design diminishes users' perceived control over their privacy and their trust in the cookie data collector, while its influence on users' privacy concerns and perceived privacy risks is more subtle and varied. Still, the overarching theme in the findings is that deceptive design led to a more negative perception of privacy compared to cookie consent requests without it, especially in terms of control and trust. Regarding users' overall

perceptions of privacy, the findings suggest that privacy is not only perceived binarily as negative or positive, or protected or compromised, but rather the perception is a flexible concept that changes based on specific deceptive patterns and the user's own habitual behavior as well as interest toward protecting their privacy. Therefore, the findings cannot be concluded into one general perception only. Still, the findings lean toward users perceiving their privacy as compromised, disregarded, and unprotected when deceptive design is included in cookie consent requests. Even if users may have learned to withstand or bypass deceptive design due to its ubiquitous nature, the general perception is that deceptive design undervalues users' privacy. Additionally, the findings of this study highlight the role of deceptive design as an influencing factor for users' overall perceptions of privacy, which has not yet been fully explored in previous research.

The findings were largely supported by previous studies, but this research uniquely looked at deceptive design's influence on users' comprehensive perceptions of privacy and took a user experience-oriented perspective in order to understand them. Lastly, even though the study shows a predominantly negative influence of deceptive design on users' perceptions of privacy, the findings are context- and design-specific and may not apply to all deceptive patterns and contexts. Still, the findings of this study, combined with findings from previous research and legislative measures, all ultimately emphasize the need to discontinue using deceptive design in cookie consent requests' user interfaces to enhance users' privacy.

By focusing on users' comprehensive perceptions of privacy, this study brings attention to the privacy implications of deceptive design and highlights the importance of adhering to privacy-protective, transparent design guidelines such as the PbD principles by Cavoukian (2010) and the Privacy Attributes by Barth et al. (2022) to ensure private and ethical online interactions and to foster positive perceptions of privacy. On a practical level, the study provides insights for designers, developers, and policymakers. As legislation already indirectly prohibits deceptive design and organizations seem to find it difficult to follow those vague guidelines, incorporating practical privacy-protective design guidelines into regulatory frameworks could help practitioners to comply with regulations in practice. This way, users' perceptions of privacy would be upheld, and the risks associated with non-transparent cookie consent requests would be minimized. Since this study strongly advocates for end users' privacy rights, the study's societal benefits are highlighted. Implementing privacy-protective design principles and strengthening legislations to explicitly prohibit deceptive design practices has direct effects on end-users as well – some possible effects could be reduced cognitive load, protected privacy rights, and increased trust in data collectors. Furthermore, with hopes of deceptive design becoming less common, users could be more carefree in their online interactions, especially regarding cookie consent requests, due to increased confidence in their privacy and more transparent data collection and handling practices.

Although the study had certain methodological and scope-related boundaries, it still contributes to the constantly expanding literature on users' perceptions of privacy and deceptive design, encouraging further studies to take a more holistic, user experience-oriented perspective on the topic of privacy. The novel framework this study proposed could be further tested in future studies and expanded to capture all areas of users' perceptions of privacy. The framework could be tested in other privacy-related contexts, and statistic research could be conducted to test other factors' influence and their significance on users' privacy perceptions. Lastly, as the findings were strongly design-specific, it could be further explored which types of deceptive patterns most influence users' perceptions and why, to be able to pinpoint specific design pain points to more precisely address any privacy-protective design guidelines.

As deceptive design remains prevalent for the time being, this study calls for industry-wide commitment to ethical, privacy-protective standards and guidelines to allow for users to use online services without compromising their privacy and feeling unempowered due to the lack of it. By further investigating, expanding and testing the theoretical framework used in this study, further research could better contribute to practice and improve users' perceptions of privacy by promoting transparency in design choices, and ultimately establish a carefree and trustworthy online environment for users.

REFERENCES

- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, 50(3), Article 44. <https://doi.org/10.1145/3054926>
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514. <https://doi.org/10.1126/science.aaa1465>
- Act 917/2014 of the Finnish Parliament. (2023). The Act on Electronic Communications Services. *Finlex*. <https://www.finlex.fi/fi/laki/ajantasa/2014/20140917>
- Adams, A. (1999). Users' perception of privacy in multimedia communication. *CHI99: Conference on Human Factors in Computing Systems, Pennsylvania, USA*, 53-54. <https://doi.org/10.1145/632716.632752>
- Alharbi, J. A., Albeshar, A. S., & Wahsheh, H. A. (2023). An empirical analysis of e-governments' cookie interfaces in 50 countries. *Sustainability*, 15(2), 1231. <https://doi.org/10.3390/su15021231>
- Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, and crowding*. Brooks/Cole.
- Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy*, 8(1), 21-27. <https://doi.org/10.1109/MSP.2010.38>
- Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138-150. <https://doi.org/10.1016/j.dss.2010.01.010>
- Barth, S., Ionita, D., & Hartel, P. (2022). Understanding online privacy – A systematic review of privacy visualizations and privacy by design guidelines. *ACM Computing Surveys*, 55(3), Article 3. <https://doi.org/10.1145/3502288>
- Beckwith, R. (2003). Designing for ubiquity: The perception of privacy. *IEEE Pervasive Computing*, 2(2), 40-46. <https://doi.org/10.1109/MPRV.2003.1203752>
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1041. <https://doi.org/10.2307/41409971>
- Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021). "I am definitely manipulated, even when I am aware of it. It's

- ridiculous!" – Dark patterns from the end-user perspective. *Proceedings of the 2021 ACM Designing Interactive Systems Conference, Virtual event, USA*, 763–776. <https://doi.org/10.1145/3461778.3462086>
- Brakus, J. J., Schmitt, B. H., & Zarantonello, L. (2009). Brand experience: What is it? How is it measured? Does it affect loyalty? *Journal of Marketing*, 73(3), 52–68. <https://doi.org/10.1509/jmkg.73.3.052>
- Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. Sage.
- Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. [deceptive.design](https://www.deceptive.design/). <https://www.deceptive.design/>
- Brignull, H. (2011, November 1). *Dark patterns: Deception vs. honesty in UI design*. A List Apart. <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/>
- Cavoukian, A. (2010). Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society*, 3(2), 247–251. <https://doi.org/10.1007/s12394-010-0062-y>
- Chang, Y., Wong, S. F., & Lee, H. (2015). Understanding perceived privacy: A privacy boundary management model. *Pacific Asia Conference on Information Systems (PACIS)*, 78. <https://aisel.aisnet.org/pacis2015/78/>
- Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 35(3), 445–459. <https://doi.org/10.1016/j.giq.2018.04.002>
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6, 181–202. <https://doi.org/10.1007/s10799-005-5879-y>
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10(1), 104–115. <https://doi.org/10.1287/orsc.10.1.104>
- Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, HI, USA*, 1–14. <https://doi.org/10.1145/3313831.3376600>
- Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents – Measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413–422. <https://doi.org/10.1080/01449290410001715723>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 1–104. <https://doi.org/10.1287/isre.1060.0080>

- Dinev, T., Heng, X., & Smith, H. J. (2009). Information privacy values, beliefs and attitudes: An empirical analysis of Web 2.0 privacy. *2009 42nd Hawaii International Conference on System Sciences, HI, USA*, 1–10.
<https://doi.org/10.1109/HICSS.2009.255>
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295–316.
<https://doi.org/10.1057/ejis.2012.23>
- 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). *Official Journal of the European Union*. L201, 37-47. <http://data.europa.eu/eli/dir/2002/58/oj>
- Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive). *Official Journal of the European Union*. L149, 22-39.
<http://data.europa.eu/eli/dir/2005/29/oj>
- Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. *Official Journal of the European Union*. L321, 36-214.
<http://data.europa.eu/eli/dir/2018/1972/oj>
- Eccles, D. W., & Arsal, G. (2017). The think aloud method: What is it and how do I use it? *Qualitative Research in Sport, Exercise and Health*, 9(4), 514-531.
<https://doi.org/10.1080/2159676X.2017.1331501>
- Eskola, J., & Suoranta, J. (2014). *Johdatus laadulliseen tutkimukseen* (10th ed.). Vastapaino.
- Federal Trade Commission. (1998). *Privacy online: A report to congress*.
<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>
- Federal Trade Commission. (2000). *Privacy online: Fair information practices in the electronic marketplace – A report to congress*.
<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>
- Finnish National Cyber Security Centre - Traficom. (n.d.). *Cookies*. Retrieved January 5, 2024, from <https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/cookies>
- Finnish Transport and Communications Agency - Traficom. (2022). *Cookies and other data stored on users' terminal devices and the use of such data – Guidelines for service providers*.
<https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regu>

lation/Guidance_on_the_use_of_web_cookies_for_the_service_providers%20%28002%29.pdf

- Flinn, S., & Lumsden, J. (2005). User Perceptions of Privacy and Security on the Web. *Third annual conference on Privacy, Security and Trust, St. Andrews, Canada*, 15-26.
- Forbrukerrådet. (2018). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. <https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf>
- Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-products and e-services. *Omega*, 32(6), 407–424. <https://doi.org/10.1016/j.omega.2004.01.006>
- Grammarly Inc. (2024) *Grammarly* [Software]. <https://www.grammarly.com>
- Graßl, P., Schraffenberger, H., Borgesius, F. Z., & Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, 3(1), 1-38. <https://doi.org/10.33621/jdsr.v3i1.54>
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Québec, Canada*, Paper 534, 1-14. <https://doi.org/10.1145/3173574.3174108>
- Gray, C. M., Chen, J., Chivukula, S. S., & Qu, L. (2021). End user accounts of dark patterns as felt manipulation. *Proceedings of the ACM on Human-Computer Interaction, NY, USA*, 5(CSCW2), Article 372, 1-25. <https://doi.org/10.1145/3479516>
- Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan*, Article 172, 1–18. <https://doi.org/10.1145/3411764.3445779>
- Ha, V., Inkpen, K., Al Shaar, F., & Hdeib, L. (2006). An examination of user perception and misconception of internet cookies. *CHI '06 Extended Abstracts on Human Factors in Computing Systems, Québec, Canada*, 833–838. <https://doi.org/10.1145/1125451.1125615>
- Habib, H., Li, M., Young, E., & Cranor, L. (2022). “Okay, whatever”: An evaluation of cookie consent interfaces. *CHI Conference on Human Factors in Computing Systems, LA, USA*, Article 621, 1–27. <https://doi.org/10.1145/3491102.3501985>
- Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., Cranor, L. F., Sadeh, N., & Schaub, F. (2019). An empirical analysis of data deletion and {opt-out} choices on 150 websites. *Fifteenth Symposium on Usable*

- Privacy and Security (SOUPS 2019)*, CA, USA, 387–406.
<https://www.usenix.org/conference/soups2019/presentation/habib>
- Hirsjärvi, S., & Hurme, H. (2017). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Gaudeamus.
- Hirsjärvi, S., Remes, P., & Sajavaara, P. (1997). *Tutki ja kirjoita* (11th ed.). Tammi.
- Interaction Design Foundation - IxDF. (2016, June 2). *What is usability testing?*
<https://www.interaction-design.org/literature/topics/usability-testing>
- Jørgensen, A. H. (1990). Thinking-aloud in user interface design: A method promoting cognitive ergonomics. *Ergonomics*, 33(4), 501-507.
<https://doi.org/10.1080/00140139008927157>
- Keleher, M., Westin, F., Nagabandi, P., & Chiasson, S. (2022). How well do experts understand end-users' perceptions of manipulative patterns? *Nordic Human-Computer Interaction Conference (NordiCHI '22)*, Aarhus, Denmark, Article 52, 1–21. <https://doi.org/10.1145/3546155.3546656>
- Koch, R. (2019, May 9). *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.EU.
<https://gdpr.eu/cookies/>
- Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the Web. *ACM Transactions on the Web*, 15(4), 1–42. <https://doi.org/10.1145/3466722>
- Krisam, C., Dietmann, H., Volkamer, M., & Kulyk, O. (2021). Dark patterns in the wild: Review of cookie disclaimer designs on top 500 German websites. *Proceedings of the 2021 European Symposium on Usable Security, Karlsruhe, Germany*, 1–8. <https://doi.org/10.1145/3481357.3481516>
- Kristol, D. M. (2001). HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology (TOIT)*, 1(2), 151–198.
<https://doi.org/10.1145/502152.502153>
- Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018). “This website uses cookies”: Users' perceptions and reactions to the cookie disclaimer. *Proceedings of the 3rd European Workshop on Usable Security, European Workshop on Usable Security, London, England*, 1-11.
<https://doi.org/10.14722/eurosec.2018.23012>
- Kulyk, O., Mayer, P., Käfer, O., & Volkamer, M. (2018). A concept and evaluation of usable and fine-grained privacy-friendly cookie settings interface. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, NY, USA, 1058–1063. <https://doi.org/10.1109/TrustCom/BigDataSE.2018.00148>
- Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of Westin's studies* (CMU-ISRI-5-138). Institute for Software Research International, Carnegie Mellon University.

- Kvale, S. (1996). *InterViews: An introduction to qualitative research interviewing*. Sage.
- Lai, P. C. (2016). Design and security impact on consumers' intention to use single platform e-payment. *Interdisciplinary Information Sciences*, 22(1), 111-122. <https://doi.org/10.4036/iis.2016.R.05>
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue – Multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22-42.
- Liu, Z., Iqbal, U., & Saxena, N. (2022). *Opted out, yet tracked: Are regulations enough to protect your privacy?* arXiv. <https://doi.org/10.48550/arXiv.2202.00885>
- Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., & Rodríguez de las Heras Ballell, T. (2022). *Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation : final report*. Publications Office of the European Union. <https://data.europa.eu/doi/10.2838/859030>
- Machuletz, D., & Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(2), 481-498. <https://doi.org/10.2478/popets-2020-0037>
- Maier, M., & Harr, R. (2020). Dark design patterns: An end-user perspective. *Human Technology*, 16(2), 170-199. <https://doi.org/10.17011/ht/urn.202008245641>
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 311-416. <https://doi.org/10.1287/isre.1040.0032>
- Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33(3), 5-21. <https://doi.org/10.1111/j.1540-4560.1977.tb01879.x>
- Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 9-17). Springer. https://doi.org/10.1007/978-3-642-21521-6_2
- Martini, M., & Drews, C. (2022). *Making choice meaningful – Tackling dark patterns in cookie and consent banners through european data privacy law*. SSRN. <https://doi.org/10.2139/ssrn.4257979>
- Mathur, A., Acar, G., Friedman, M. J., 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*, 3(CSCW), Article 81, 1-32. <https://doi.org/10.1145/3359183>
- Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What makes a dark pattern... dark? Design attributes, normative considerations, and measurement

methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan*, Article 360, 1–18.
<https://doi.org/10.1145/3411764.3445610>

- Matte, C., Bielova, N., & Santos, C. (2020). Do cookie banners respect my choice? : Measuring legal compliance of banners from IAB Europe’s transparency and consent framework. *2020 IEEE Symposium on Security and Privacy (SP), CA, USA*, 791–809.
<https://doi.org/10.1109/SP40000.2020.00076>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709–734.
<https://doi.org/10.2307/258792>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 227–359.
<https://doi.org/10.1287/isre.13.3.334.81>
- Mejtoft, T., Frängsmyr, E., Söderström, U., & Norberg, O. (2021). Deceptive design: Cookie consent and manipulative patterns. In A. Pucihar, M. Kljajić Borštnar, R. Bons, H. Cripps, A. Sheombar & D. Vidmar (Eds.), *34th Bled eConference Digital Support from Crisis to Progressive Change: Conference Proceedings* (pp. 397–408). University of Maribor Press.
<https://doi.org/10.18690/978-961-286-485-9.29>
- Mejtoft, T., Vejbrink Starbrink, N., Roos Morales, C., Norberg, O., Andersson, M., & Söderström, U. (2023). Cookies and trust: Trust in organizations and the design of cookie consent prompts. *Proceedings of the European Conference on Cognitive Ergonomics 2023, Swansea, United Kingdom*, Article 18, 1–6. <https://doi.org/10.1145/3605655.3605668>
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & 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, HI, USA*, 1–13.
<https://doi.org/10.1145/3313831.3376321>
- OpenAI. (2024a). *ChatGPT* (GPT-4 model) [Large language model].
<https://openai.com/chatgpt>
- OpenAI. (2024b). *Scholar GPT* (AI language model) [Software].
<https://openai.com>
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134.
<https://doi.org/10.1080/10864415.2003.11044275>
- Pedersen, D. M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, 19(4), 397–405.
<https://doi.org/10.1006/jevp.1999.0140>

- Perttula, J. (1995). *Kokemus psykologisena tutkimuskohteena: johdatus fenomenologiseen psykologiaan*. Suomen fenomenologinen instituutti.
- Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, 13(1), 6–14. <https://doi.org/10.1080/15267431.2013.743426>
- Petronio, S. (2016). Communication privacy management. In K.B. Jensen, E.W. Rothenbuhler, J.D. Pooley & R.T. Craig (Eds.), *The International Encyclopedia of Communication Theory and Philosophy* (pp. 1–9). John Wiley & Sons, Inc. <https://doi.org/10.1002/9781118766804.wbiect138>
- Pettersson, I., Lachner, F., Frison, A.-K., Riener, A., & Butz, A. (2018). A bermuda triangle? A review of method application and triangulation in user experience evaluation. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Québec, Canada, Paper 461*, 1–16. <https://doi.org/10.1145/3173574.3174035>
- Posner, R. A. (1981). The economics of privacy. *The American Economic Review*, 71(2), 405–409.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1-88. <http://data.europa.eu/eli/reg/2016/679/oj>
- Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act). *Official Journal of the European Union*. L265, 1-66. <http://data.europa.eu/eli/reg/2022/1925/oj>
- San Martín, S., & Camarero, C. (2009). How perceived risk affects online buying. *Online Information Review*, 33(4), 629-654. <https://doi.org/10.1108/14684520910985657>
- Santos, C., Nouwens, M., Toth, M., Bielova, N., & Roca, V. (2021). Consent management platforms under the GDPR: Processors and/or controllers? In N. Gruschka, L. F. C. Antunes, K. Rannenber, & P. Drogkaris (Eds.), *Privacy Technologies and Policy* (pp. 47–69). Springer. https://doi.org/10.1007/978-3-030-76663-4_3
- SciSpace. (2024). *SciSpace* [Software]. Pubgenius Inc. <https://www.scispace.com>
- Singh, A. K., Upadhyaya, N., Seth, A., Hu, X., Sastry, N., & Mondal, M. (2022). What cookie consent notices do users prefer: A study in the wild. *Proceedings of the 2022 European Symposium on Usable Security, Karlsruhe, Germany*, 28–39. <https://doi.org/10.1145/3549015.3555675>
- Smith, Dinev, & Xu. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015. <https://doi.org/10.2307/41409970>

- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196. <https://doi.org/10.2307/249477>
- Soe, T. H., Nordberg, O. E., 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, Tallinn, Estonia*, Article 19, 1-12. <https://doi.org/10.1145/3419249.3420132>
- Tan, W. S., Liu, D., & Bishu, R. (2009). Web evaluation: Heuristic evaluation vs. user testing. *International Journal of Industrial Ergonomics*, 39(4), 621-627. <https://doi.org/10.1016/j.ergon.2008.02.012>
- Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Tammi. (Original work published 2002)
- University of Jyväskylä. (n.d.). *Using AI-based applications in studies – JYU's instructions and guidelines*. Retrieved November 3, 2024, from <https://www.jyu.fi/en/for-students/instructions-for-bachelors-and-masters-students/regulations-and-directives-guiding-studies/using-ai-based-applications-in-studies-jyus-instructions-and-guidelines>
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, United Kingdom*, 973-990. <https://doi.org/10.1145/3319535.3354212>
- Waldo, J., Lin, H. S., & Millett, L. I. (2010). Engaging privacy and information technology in a digital age: Executive summary. *Journal of Privacy and Confidentiality*, 2(1), 5-18. <https://doi.org/10.29012/jpc.v2i1.580>
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.
- Westin, A. (1967). *Privacy and freedom*. Athenaeum.
- Westin, A. F. (2003). Social and political dimensions of privacy: Social and political. *Journal of Social Issues*, 59(2), 431-453. <https://doi.org/10.1111/1540-4560.00072>
- Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), 798-824. <https://doi.org/10.17705/1jais.00281>

APPENDIX 1 OUTLINE FOR USER TESTING AND INTERVIEWS

INTRODUCTION

- Myself, my field of study, and research interests.
- The structure of the research setting.
- Practical information about the research.
- Introducing the research topic, purpose, and goal.

RECORDING BEGINS

BACKGROUND INFORMATION

1. COOKIES

- a) How would you explain cookies, as well as how they function and what is their purpose? Tell freely.
 - a. Tell more information to the participant if needed.
- b) How often do you encounter cookie consent requests?
- c) What types of cookie consent request designs have you encountered? Can you specify certain style patterns?
- d) General questions
 - a. How often do you visit websites?
 - b. How often do you encounter a cookie consent request when visiting websites?
- e) Some questions from the UTAUT2 model (Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 157-178.)
 - a. Expectations for using cookies
 - i. *Do you find cookies useful in your daily life?*
 - ii. *Do you think cookies helps you accomplish things more quickly?*
 - iii. *Do you think cookies increase your productivity?*
 - b. Effort needed for using cookie consent requests
 - i. *Is learning how to use cookie consent requests easy for you?*
 - ii. *Is your interaction with cookie consent requests clear and understandable?*
 - iii. *Is it easy for you to become skillful at using cookie consent requests?*
 - c. Facilitating conditions
 - i. *Do you have the resources needed for using cookie consent requests?*
 - ii. *Do you have the knowledge necessary to use cookie consent requests?*
 - iii. *Can you get help from others when you have difficulty using cookie consent requests?*
 - d. Hedonic motivation
 - i. *Do you think using cookie consent requests is fun / enjoyable / entertaining?*
 - e. Habit
 - i. *Have you formed a habit for using cookie consent requests?*
 - ii. *Do you think it is voluntary to use cookie consent requests?*

2. PRIVACY

- a) What does privacy mean to you, for example, when you visit a website and cookie data is collected of you?
- b) How much do you know about privacy and what it entails? Tell freely.
 - Tell more information to the participant if needed.

- c) Questions from Xu et al. (2011, Appendix B)
- Disposition to value privacy
 - *Compared to others, are you more sensitive about the way companies handle your personal information?*
 - *Is it the most important thing to you to keep your information private?*
 - *Compared to others, do you tend to be more concerned about threats to your information privacy?*
 - Privacy awareness
 - *Are you aware of the privacy issues and practices in our society?*
 - *Do you follow the news and developments about the privacy issues and privacy violations?*
 - *Do you keep yourself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy?*
 - Previous privacy experience (ask to not be too personal when answering)
 - *How often have you been a victim of what you felt was an improper invasion of privacy?*
 - *How much have you heard or read during the past year about potential misuse of information collected from the Internet?*
 - *How often have you experienced incidents where your personal information was used by a company without your authorization?*

1. DECEPTIVE DESIGN

- a) Explain the concept of deceptive design and deceptive patterns to the participant.
- b) When did you last encounter deceptive patterns?
- c) Could you give some examples of the types of deceptive patterns you have encountered on websites or on cookie consent requests?

2. GENERAL

- a) How would you describe your level of technological knowledge and skills?

POSSIBILITY TO ASK QUESTIONS OR GIVE OTHER COMMENTS

USER TESTS + THINK-ALOUD

- Information about how this part is conducted and what is required from the participant

PARTICIPANT'S SCREEN IS SHARED

- 1ST PRACTICE USER TEST
 - Link: <https://www.jyu.fi/fi>
 - Goal: *From the University of Jyväskylä's website, find the principal's name.*
- 2ND PRACTICE USER TEST
 - Link: <https://www.kyberturvallisuuskeskus.fi/fi>
 - Goal: *From the Finnish National Cyber Security Centre's (Traficom) website, find the instructions for ensuring the security of your mobile phone, targeted for private individuals.*
- 3RD PRACTICE USER TEST
 - Link: <https://www.kela.fi/henkiloasiakkaat>
 - Goal: *From Kela's website, find the amount of the healthcare fee that students need to pay.*
- 1ST OFFICIAL USER TEST
 - Goal: *Complete the cookie consent request and get to the front page of the mock-up website.*
 - When completed, tell the participant what deceptive pattern types this mock-up had.

- **2ND OFFICIAL USER TEST**
 - Same as previous.
- **3RD OFFICIAL USER TEST**
 - Same as previous.

PARTICIPANT'S SCREEN SHARING STOPS

INTERVIEW

1. **THEME: PRIVACY CONCERNS**

- a) Do cookies or cookie consent requests awaken concerns about your privacy?
- b) Does deceptive design, used in cookie consent requests, awaken concerns about your privacy?
- c) What kind of concerns? Why these concerns? Where could these concerns lead to, in the worst-case scenario?
- d) How do these concerns affect your perception of privacy?
- e) Practical examples or experiences related to these concerns?
- f) How could design reduce or eliminate these concerns? Or could it?

2. **THEME: CONTROL OVER PRIVACY**

- a) What does control mean to you when it comes to the collection of your cookie data?
- b) Do you think or do you know that you can control your own privacy and the sharing of your data in cookie consent requests?
- c) Additional questions from Xu et al. (2011, appendix B)
 - *Do you think that you can control who has access to your information that the website collects?*
 - *Do you think that you can control what kind of information the website collects of you?*
 - *Do you think that you can control how the website uses your information?*
 - *Do you think that you have control or decision-making power over your own information even after you have already shared the information with the website?*
- d) How much control do you feel that you have over your privacy when using cookie consent requests?
- e) Do you think that deceptive design affects your possibilities to control your privacy? How? What kind of deceptive patterns?
- f) How does the perception of control affect your perception of privacy?
- g) Practical experiences or examples related to control?
- h) Fair Information Practice Principles (FIPs):
 - **Choice:** *Do you feel that you have the freedom of choice (voluntariness) to decide who you share your cookie information with, especially when deceptive design is used in the request?*
 - **Access:** *Do you feel that deceptive design affects your ability to access, edit and delete the cookie data collected about you, if necessary?*
 - **Security:** *Do you feel that deceptive design affects how well and to what extent you are informed about the privacy of the processing and sharing of your data?*
 - **Enforcement:** *Do you feel that a cookie data collector who uses deceptive design would stand behind their own actions and be responsible for their own actions if they violated privacy laws?*

3. **THEME: TRUST IN THE COOKIE DATA COLLECTOR**

- a) How would you define trust? How about a practical example of it?
- b) Do you normally trust an organization that collects cookie data of you?
- c) Do you / would you trust them if they use deceptive design in their cookie consent request?
- d) How does deceptive design affect your trust in the cookie data collector?
- e) How does trust affect your perception of privacy?

- f) When do you think that the level of trust is enough for you to trust the cookie data collector and for you to share data with them? Which factors might affect the trust (brand, design, previous experiences...)?
- g) How does legislation affect your trust? Do you believe that it has an effect? Do you trust that the data collector obeys the legislation?
- h) How could design enhance trust?
- i) Practical experiences or examples of trust in the context of cookie consent requests?
- j) Mayer et al. (1995) 3 levels of trust. When deceptive design is used...
 - o **Ability:** ... do you think that the cookie data collector is capable of performing this task of collecting cookie data?
 - o **Benevolence:** ...do you feel that the cookie data collector is acting with good intentions?
 - o **Integrity:** ...do you feel that the cookie data collector is acting honestly with regard to the collection of cookie data?
- k) Gefen & Straub (2004)
 - o **Predictability:** Do you feel that the cookie data collector's behavior is predictable, without you having to worry about what happens after your data is shared with them?
- l) McKnight et al. (2002)
 - o **Institution-based trust:** What is your general level of trust in, for example, the internet and technology in general, both regarding their operation and the legislation related to them?

4. THEME: PERCEIVED PRIVACY RISKS

- a) What kind of risks do you generally find there to be for collecting, using and sharing your personal information?
- b) Do you think that there are some risks related to the collection of your cookie data? What kind of risks?
- c) Xu et al. (2011, appendix B) – When deceptive design is used...
 - o ...would it be risky to give your cookie information to that website?
 - o ...would there be high potential for privacy loss associated with giving cookie information to that website?
 - o ...could your cookie information be inappropriately used by that website?
 - o ... would providing that website with your cookie information involve many unexpected problems?
- d) How big or significant do you think these risks are?
 - o Questions to help understand this better: (how much) do you worry about them / which of them is the worst or least bad / what would be the worst-case scenario if these risks would realize / what kind of personal information would be the worst to be leaked or used wrongly?
- e) Do you think that using deceptive design in cookie consent requests increases / reduces risks related to your privacy? Does deceptive design bring out some other risks that would not occur otherwise?
- f) Does deceptive design make the risks either worse or better?
- g) How could design reduce privacy risks?
- h) How do risks affect your perception of privacy?
- i) Practical experiences or examples of privacy risks in cookie consent requests?
- j) Privacy calculus (Dinev & Hart, 2006)
 - o When making a decision to either accept or decline the collection of cookie data, do you somehow balance the possible benefits with the risks?
 - o What kind of benefits do you think cookie data / deceptive design can provide you?

5. THEME: PRIVACY BY DESIGN

- a) Which types of deceptive patterns do you remember from the user tests? And what types of deceptive patterns have you encountered on actual websites' cookie consent requests (experiences and examples about them)?
- b) Have you noticed that you would make different choices than you would normally make with the guidance of deceptive design?

- c) Does deceptive design affect your way of operating a cookie consent request?
- d) What kind of feelings and thoughts does deceptive design awaken in you? What is your opinion on deceptive design? Give examples.
- e) Does deceptive design bring you something positive or benefits?
- f) Does deceptive design affect your perception of privacy? How does it affect? How much does it affect (and what affects more or less than it)?
- g) What kind of (visual) design elements could affect this perception?
- h) What kind of design makes a cookie consent request privacy-protective and what kind of design makes it less privacy-protective?
- i) How could design make the perception of privacy better in cookie consent requests?
- j) A power point slide containing Privacy attributes by Barth et al. (2022) is shown.
 - o Here you can see key words related to design and privacy.
 - i. *Accountability, anonymization, data collection, control, correctness, disclosure, functionality, purpose, pseudonymization, storing/retention, the right to be forgotten, sale, security, sharing, transparency.*
 - o Which of these attributes do you relate to cookie consent requests? Which ones not?
 - o Do some of these attributes emerge better, or too much, than others? What about too little?
 - o Does deceptive design affect the appearance of some of these in cookie consent request?
 - o Which of these attributes would be especially important to take into account in a cookie consent request?

CONCLUSION

1. Normal cookie consent requests

- a) How would you rate your overall perception of the privacy of cookie consent requests?
 - o Scale of 1 – 5 (1: not private, 5: very private)
- b) What are your overall feelings about the privacy of cookie consent requests?
 - o Scale 1 – 5 (1: very negative, 3: neutral, 5: very positive)

2. Cookie consent requests that use deceptive design

- a) How would you rate your overall perception of the privacy of cookie consent requests that use deceptive design?
 - o Scale of 1 – 5 (1: not private, 5: very private)
- b) What are your overall feelings about the privacy of cookie consent requests that use deceptive design?
 - o Scale 1 – 5 (1: very negative, 3: neutral, 5: very positive)

FINISHING UP

1. Anything else that comes to mind related to the topics or user tests?

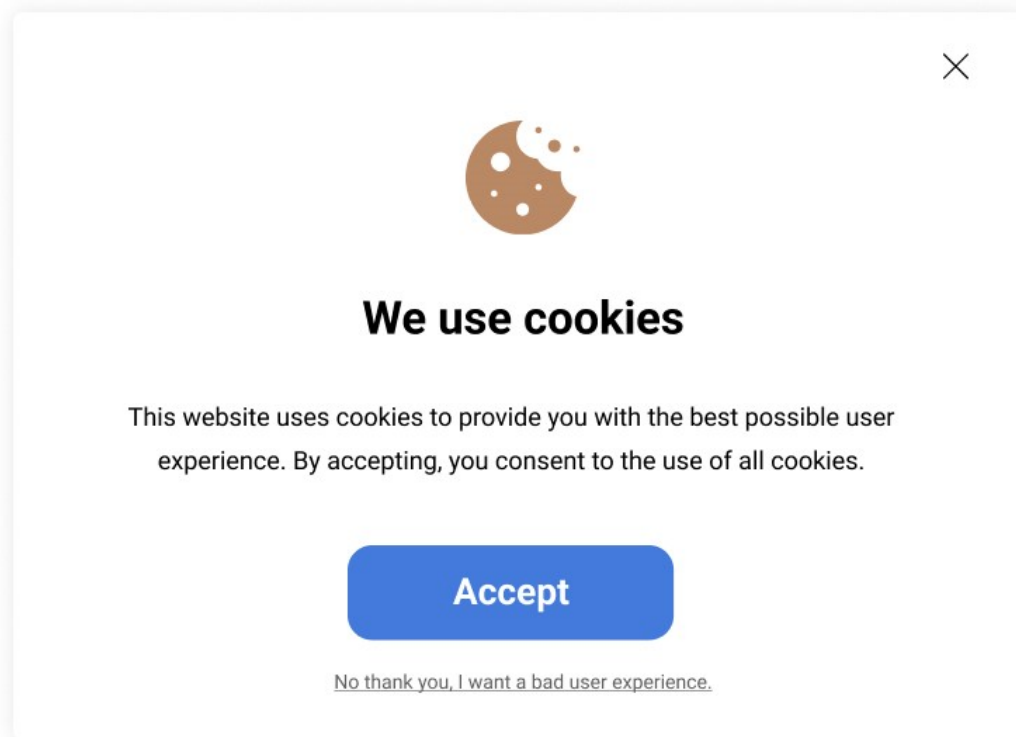
RECORDING ENDS

2. Any other questions or comments related to the research?
3. A thank you and a reminder that the participant can still at any point cancel their participation to the research.

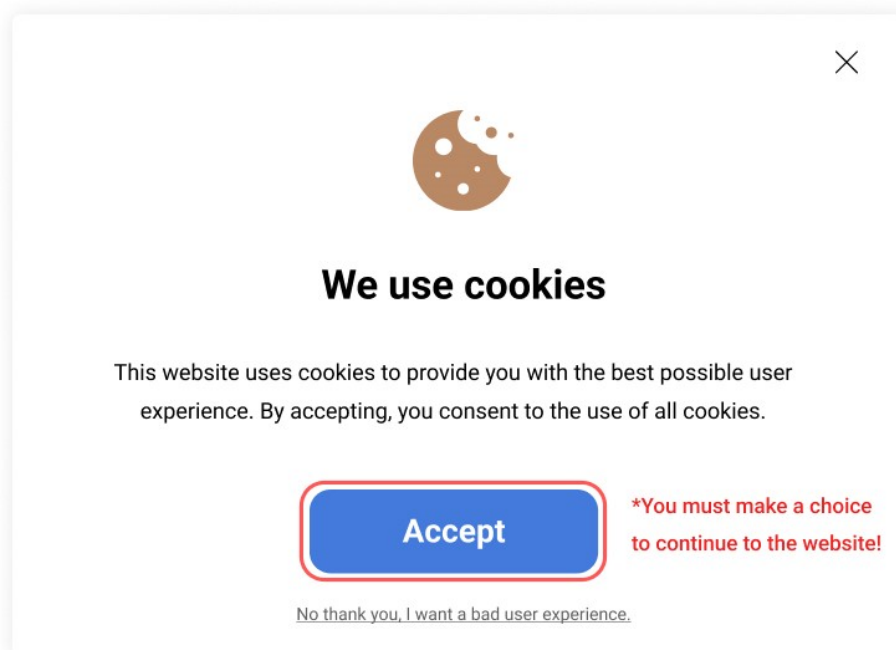
APPENDIX 2 MOCK-UPS FOR USER TESTING

USER TEST 1 – MOCK-UP 1

Frame 1: start




Frame 2: error from clicking on the X in the top right corner



USER TEST 2 – MOCK-UP 2

Frame 1: start




We use cookies

On this website, cookies are used to ensure the functionality of the website, for statistical and analytical purposes, and to personalise content and marketing. By accepting all cookies, you ensure the functionality of the site and the best user experience. You can change your cookie preferences in the settings.
[Read more about privacy policy and cookies.](#)

[Settings](#)

Frame 2: settings




Cookie settings

- Essential cookies**
 These enable functionalities that are essential for using the site, such as logging into secure parts of the site, remembering the contents of your shopping cart in online shops, filling in forms or improving security.
- Functional cookies**
 These cookies are used to enhance and improve the functionality of the website, but they are not strictly necessary to use the site.
- Personalization cookies**
 These cookies make it possible, for example, to remember the choices you make on a page, such as language and font size, or your username and password between visits to the site.
- Marketing cookies**
 For example, these cookies can be used to collect information about your interests based on your online behaviour and to show you targeted advertisements based on this information.

[Read more about privacy policy and cookies.](#)
[Save settings](#)

Frame 3: error when de-selecting essential cookies



Cookie settings

- Essential cookies** *You must accept at least the essential cookies to continue on the site!
 These enable functionalities that are essential for using the site, such as logging into secure parts of the site, remembering the contents of your shopping cart in online shops, filling in forms or improving security.
- Functional cookies**
 These cookies are used to enhance and improve the functionality of the website, but they are not strictly necessary to use the site.
- Personalization cookies**
 These cookies make it possible, for example, to remember the choices you make on a page, such as language and font size, or your username and password between visits to the site.
- Marketing cookies**
 For example, these cookies can be used to collect information about your interests based on your online behaviour and to show you targeted advertisements based on this information.

[Read more about privacy policy and cookies.](#)
[Save settings](#)

USER TEST 3 - MOCK-UP 3

Frame 1: start



Our site uses cookies

Essential cookies (consent required)

These enable functionalities that are essential for using the site, such as logging into secure parts of the site, remembering the contents of your shopping cart in online shops, filling in forms or improving security.

Functional cookies

These cookies are used to enhance and improve the functionality of the website.

Personalization cookies

These cookies make it possible, for example, to remember the choices you make on a page, such as language and font size, or your username and password between visits to the site.

Marketing cookies

For example, these cookies can be used to collect information about your interests based on your online behaviour and to show you targeted advertisements based on this information.

[Read more about privacy policy and cookies.](#)

[Save settings](#)

Accept all

APPENDIX 3 INFORMATION LEAFLET FOR PARTICIPANTS

JYVÄSKYLÄN YLIOPISTO

INFORMAATIOTEKNOLOGIAN
TIEDEKUNTA

Pvm 26.3.2024

TIEDOTE KOSKIEN OPISKELIJAN TEKEMÄÄ TUTKIMUSTA

1. Pro gradu -tutkielma ja pyyntö osallistua

Sinua pyydetään mukaan Noora Tuokkolan tietojärjestelmätieteen pro gradu -tutkimukseen, jossa tutkitaan sinun havaintojasi, ajatuksiasi, tunteitasi ja kokemuksiasi liittyen verkkosivuilla käytettyjen evästepepyntöjen yksityisyyteen. Erityisenä tarkastelukohteena on evästepepyntöjen harhaanjohtava muotoilu. Ennakkokyselyn avulla kerään tietoina nimesi, ikäsi, sukupuolesi, koulutustasosi ja koulutusalasasi sekä yhteystietosi.

Sinua pyydetään osallistumaan, koska olet ilmoittautunut halukkaaksi osallistumaan tutkimukseen ja sovit kohderyhmään.

Osallistuminen edellyttää, että olet:

- a) törmännyt evästepepyntöön verkkosivulla viimeisen 1 kuukauden aikana,
- b) syntynyt Z-sukupolven vuosina 1995-2010
- c) ja olet korkeakoulutettu tai korkeakouluopiskelija.

Tämä tiedote kuvaa opinnäytetyötä ja siihen osallistumista. Toisessa saamassasi liitteessä on kerrottu henkilötietojesi käsittelystä.

Tutkimus suoritetaan yksilöittäin, kokonaisuudessaan noin kymmenen (10) osallistujan kanssa.

Tämä on yksittäinen opinnäytetyö, eikä sinuun oteta myöhemmin uudestaan yhteyttä.

Ohjaajana toimii Tiina Koskelainen, [sähköpostiosoite].

2. Vapaaehtoisuus

Tähän opinnäytetyöhön osallistuminen on vapaaehtoista. Voit kieltäytyä osallistumasta, keskeyttää osallistumisen tai peruuttaa jo antamasi suostumuksen syytä ilmoittamatta milloin tahansa tutkimuksen aikana. Tästä ei aiheudu sinulle kielteisiä seurauksia.

Peruuttaessasi suostumuksesi henkilötietojesi käsittelyyn, sinusta siihen mennessä kerättyjä henkilötietoja, näytteitä ja muita tietoja ei voida käsitellä, vaan ne hävitetään, mikäli niiden poistaminen aineistosta on mahdollista.

3. Tutkimuksen kulku

Tutkimus toteutetaan käytettävyydestauksena ja teemahaastatteluna. Testaus ja haastattelu järjestetään samassa tutkimustilanteessa ja arvioitu kesto sille on noin 2 tuntia. Ennen tutkimushetkeä pyydän sinua vastaamaan sähköpostiisi lähetettyyn ennakkokyselyyn ja antamaan suostumuksesi sekä henkilötietojesi käsittelemiseen että tutkimukseen osallistumiseen. Ennakkokyselyyn vastaaminen kestää noin 5 minuuttia.

Tutkimus toteutetaan yksilöhaastatteluna ja etäyhteydellä, Microsoft Teamsin avulla. Tarvitset tutkimusta varten oman tietokoneen ja valitsemasi selaimen, jonka kautta pääset tekemään lyhyet käytettävyydestit. Käytettävyydestien aikana sinun tulee ajatella ääneen spontaanisti sanoittaen esimerkiksi omia ajatuksiasi, odotuksiasi, mielipiteitäsi, suunnitelmiasi ja epäilyksiäsi, jotka nousevat esiin käytön aikana. Käytettävyydestiä ja ääneen ajattelua harjoitellaan ennen virallisia testejä muutamalla epävirallisella harjoituksella.

Virallisissa käytettävyydesteissä pääset kokeilemaan muutamaa erilaista evästepyyntöä simulaatiosivustolla. Minkäänlaista eväsetietoa sinusta ei tutkimuksessa tallenneta. Testeissä pyydän sinua toteuttamaan selkeän ja yksinkertaisen tehtävän, jonka toteutettuasi jatkamme seuraavaan testiin. Testien tarkoitus on lähinnä palautella mieleen erilaisia evästepyyntöjen muotoilutyylejä samalla omia ajatuksiasi ääneen puhuen – en esimerkiksi tule arvioimaan testien aikana tekemiäsi valintoja. Käytettävyydestit eivät myöskään kerää sinusta eväsetietoja, sillä ne ovat vain visuaalisia prototyyppisiä verkkosivuja.

Käytettävyydestien jälkeen toteutetaan haastattelu, jossa käydään läpi muutamia eri yksityisyyteen vaikuttavia teemoja. Tarkoitus on selvittää havaintojasi, ajatuksiasi ja kokemuksiasi liittyen näihin teemoihin, ja lopulta pyrkiä muodostamaan kooste näistä. Tutkimuksen aluksi käymme lisäksi läpi muutamia haastattelukysymyksiä liittyen tutkimuksen käsitteiden ymmärtämiseen sekä teknologisiin tietoihisi ja taitoihisi.

Haastattelujen jälkeen kerätty aineisto anonymisoidaan, litteroidaan ja analysoidaan, minkä jälkeen siitä koostetaan tutkimuksen kannalta oleellista tietoa. Tutkimusmenetelmät, aineisto, analyysi ja tulokset esitetään osana pro gradu -tutkielmaa. Anonymisoitua aineistoa ja tietoja voidaan käyttää myös mahdollisiin Noora Tuokkolan toteuttamiin jatkotutkimuksiin tai muihin tieteellisiin julkaisuihin.

4. Tutkimuksesta mahdollisesti aiheutuvat hyödyt

Tutkimukseen osallistumisesta ei ole sinulle tutkittavana hyötyä. Voit kuitenkin oppia aiheista lisää ja voin halutessasi jälkikäteen toimittaa sinulle esimerkiksi lisätietoja oman yksityisyytesi suojaamiseen liittyen.

Tutkimuksesta on yleisesti hyötyä tieteelle ja yhteiskunnalle, sekä sitä kautta yksittäisille verkkosivujen käyttäjille. Tutkimuksen myötä voidaan kehittää evästepyyntöjen sisältöön ja visuaalisen muotoiluun liittyviä käytänteitä ja ohjeita, sekä mahdollisesti myös yksityisyyteen liittyvää lainsäädäntöä siihen suuntaan, että käyttäjien havainto yksityisyydestä olisi parempi. Lisäksi jatkotutkimus voi hyödyntää tässä opinnäytetyössä löydettyjä tärkeitä havaintoja.

5. Tutkimuksesta mahdollisesti aiheutuvat riskit, haitat ja epämukavuudet sekä niihin varautuminen

Tutkimukseen osallistumisesta ei odoteta aiheutuvan riskejä, haittoja tai epämukavuuksia.

6. Osallistumisen kustannukset ja korvaukset

Osallistumisesta ei makseta palkkiota eikä korvausta. Osallistuminen on maksutonta.

7. Tulokset

Henkilötietojen käsittelyn tarkoituksena on opinnäytetyön tekeminen ja valmistuminen. Opinnäytetyö julkaistaan JYX julkaisuarkistossa ja opintotehtävän arvostelee sekä ohjaaja että toinen ulkopuolinen arvioija yliopistolta. Tutkimustuloksia ei erikseen anneta tutkittaville, mutta JYX julkaisuarkistossa se on vapaasti saatavilla kaikille.

Osallistujia ei voida tunnistaa tutkimuksen tuloksista tai julkaistusta opinnäytetyöstä, sillä tiedot anonymisoidaan heti materiaalin litteroinnin yhteydessä eikä tutkittavaa voida täten tunnistaa. Tuloksissa saatetaan eritellä vastauksia eri syntymävuosien, sukupuolien, koulutuksen tasojen, koulutusalojen sekä teknologiatottumusten ja -kokemusten perusteella. Näistäkään ei yksittäistä osallistujaa voi tunnistaa, mutta tiedot ovat olennaisia tulosten kannalta.

Lisätietojen antajan yhteystiedot

Noora Tuokkola
[puhelinnumero]
[sähköpostiosoite]

APPENDIX 4 PRIVACY NOTICE FOR PARTICIPANTS

INFORMAATIOTEKNOLOGIAN
TIEDEKUNTA

Pvm 26.3.2024

TIETOSUOJAIMOITUS

Olet osallistumassa Jyväskylän yliopiston opiskelijan tekemään opinnäytetyöhön. Tässä tietosuojailmoituksessa sinulle kerrotaan henkilötietojesi käsittelystä. Sinulla on lain mukaan oikeus saada nämä tiedot.

1. Rekisterinpitäjä

Noora Tuokkola, [sähköpostiosoite], [puhelinnumero]

2. Työnohjaaja opinnäytetyössä

Tiina Koskelainen, tietojärjestelmätieteen tutkinto-ohjelmavastaava, [sähköpostiosoite], [puhelinnumero]

3. Henkilötietojen käsittelijä(t)

Seuraavia henkilötietojen käsittelijöitä käytetään:
Microsoftin O365-palvelut: OneDrive ja Teams
Webropol kyselyohjelmisto, Webropol Oy

Tietojasi käsitellään luottamuksellisesti eikä niitä luovuteta sivullisille.

Tietoihisi on kuitenkin pääsy työnohjaajalla, koska hän arvostelee, neuvoo ja ohjaa vielä keskeneräistä työtä, joka voi sisältää henkilötietojasi. Aineisto anonymisoidaan litterointivaiheessa, eikä sinua voi tässä vaiheessa enää tunnistaa aineiston perusteella.

4. Käsiteltävät henkilötiedot

Henkilötietojasi käsitellään tiedotteessa kuvattua tarkoitusta varten.

Sinusta kerätään seuraavia henkilötietoja: nimi, sähköpostiosoite, puhelinnumero, syntymävuosi, sukupuoli, koulutuksen taso, koulutusala, äänitallenne, ruudunkaappaustallenne ja haastatteluvastaukset.

Erityisiä henkilötietoryhmiä ei käsitellä.

Kaikki osallistujat ovat täysi-ikäisiä.

5. Henkilötietojen käsittelyn oikeudellinen peruste

Tutkimuksen henkilötietojen käsittely perustuu tieteellisen tutkimuksen mukaiseen yleiseen etuun (tietosuoja-asetuksen artikla 6.1.a).

Rekisteröidyille on toimitettu tämä ilmoitus sähköpostitse liitteenä tutkimuskutsun yhteydessä ja tietosuojailmoitus sekä suostumus tutkimukseen on pyydetty hyväksymään Webropol -kyselylomakkeen kautta.

6. Henkilötietojen siirto EU/ETA ulkopuolelle

Tietojasi ei siirretä EU/ETA -alueen ulkopuolelle.

7. Henkilötietojen suojaaminen

Henkilötietojen käsittely tässä tutkimuksessa perustuu asianmukaiseen tutkimussuunnitelmaan ja tutkimuksella on vastuuhenkilö. Tutkimuksen rekisteriin tallennetaan vain tutkimuksen tarkoituksen kannalta välttämättömiä tietoja. Haastatteluaineistoa käsitellään luottamuksellisesti eikä nimiä, suoria tunnistetietoja tai vastaavia julkaista tutkielmassa.

Aineisto anonymisoidaan aineiston perustamisvaiheessa (kaikki tunnistetiedot poistetaan täydellisesti, jotta paluuta tunnistelliseen tietoon ei ole eikä aineistoon voida yhdistää uusia tietoja).

Käsiteltävät henkilötiedot säilytetään tietoturvallisesti ja suojataan käyttäjätunnuksella ja salasanalla sekä Microsoftin O365 -palveluissa lisäksi kaksivaiheisella tunnistautumisella.

8. Henkilötietojen käsittelyn elinkaari

Henkilörekisteri hävitetään arviolta 12.2024 mennessä tai opinnäytetyön valmistuttua. Anonymisoitua aineistoa ja tietoja voidaan käyttää pro gradu -tutkielman lisäksi myös Noora Tuokkolan muihin mahdollisiin jatkotutkimuksiin ja tieteellisiin julkaisuihin.

9. Rekisteröidyn oikeudet

Suostumuksen peruuttaminen (tietosuoja-asetuksen 7 artikla)

Sinulla on oikeus peruuttaa antamasi suostumus, mikäli henkilötietojen käsittely perustuu suostumukseen. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritettun käsittelyyn lainmukaisuuteen.

Oikeus saada pääsy tietoihin (tietosuoja-asetuksen 15 artikla)

Sinulla on oikeus saada tieto siitä, käsitelläänkö henkilötietojasi ja mitä henkilötietojasi käsitellään. Voit myös halutessasi pyytää jäljennöksen käsiteltävistä henkilötiedoista.

Oikeus tietojen oikaisemiseen (tietosuoja-asetuksen 16 artikla)

Jos käsiteltävissä henkilötiedoissasi on epätarkkuuksia tai virheitä, sinulla on oikeus pyytää niiden oikaisua tai täydennystä.

Oikeus tietojen poistamiseen (tietosuoja-asetuksen 17 artikla)

Sinulla on oikeus vaatia henkilötietojesi poistamista tietyissä tapauksissa.

Oikeus käsittelyn rajoittamiseen (tietosuoja-asetuksen 18 artikla)

Sinulla on oikeus henkilötietojesi käsittelyn rajoittamiseen tietyissä tilanteissa kuten, jos kiistät henkilötietojesi paikkansapitävyyden.

Vastustamisoikeus (tietosuoja-asetuksen 21 artikla)

Sinulla on oikeus vastustaa henkilötietojesi käsittelyä, jos käsittely perustuu oikeutettuun etuun.

Oikeuksista poikkeaminen

Tässä kuvatuista oikeuksista saatetaan tietyissä yksittäistapauksissa poiketa tietosuoja-asetuksessa ja Suomen tietosuojalaissa säädetyillä perusteilla siltä osin, kuin oikeudet estävät tieteellisen tai historiallisen tutkimustarkoituksen tai tilastollisen tarkoituksen saavuttamisen tai vaikeuttavat sitä suuresti. Tarvetta poiketa oikeuksista arvioidaan aina tapauskohtaisesti. Oikeuksista voidaan poiketa myös, jos rekisteröityä ei pystytä tai ei enää pystytä tunnistamaan.

Profilointi ja automatisoitu päätöksenteko

Tutkimuksessa henkilötietojasi ei käytetä automaattiseen päätöksentekoon.

Rekisteröidyn oikeuksien toteuttaminen

Jos sinulla on kysyttävää rekisteröidyn oikeuksista, voit olla yhteydessä rekisterinpitäjään (ks. kohta 1).

Tietoturvaloukkauksesta tai sen epäilystä ilmoittaminen

Sinulla on oikeus tehdä valitus erityisesti vakinaisen asuin- tai työpaikkasi sijainnin mukaiselle valvontaviranomaiselle, mikäli katsot, että henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuoja-asetusta (EU) 2016/679. Suomessa valvontaviranomainen on tietosuojavaikuttettu. Tietosuojavaikuttetun toimiston ajantasaiset yhteystiedot: <https://tietosuoja.fi/etusivu>.