Deceptive Design in Cookie Consent Requests: A User-Centered Perspective on Privacy

Noora Tuokkola[1,*], Tiina Koskelainen[1], Laura Havinen[2] and Rebekah Rousi[1,2]

[1]*University of Jyväskylä, Seminaarinkatu 15, Pl 35, 40014 Jyväskylä, Finland*
[2]*University of Vaasa, Wolffintie 32, Pl 700, 65200 Vaasa, Finland*

Abstract

This study explores how users perceive their privacy in cookie consent requests that feature deceptive patterns, and the role of deceptive design in shaping these perceptions. It proposes a theory-informed analytical framework synthesizing four key factors influencing privacy perceptions: privacy concerns, control over privacy, trust in data collectors, and privacy risks. Using method triangulation – combining user testing, think-aloud protocol, and thematic interviews - the empirical study adopts a user-centered perspective. The findings reveal a predominantly negative influence of deceptive design on privacy perceptions. Although users may have learned to withstand or bypass deceptive patterns, their perceptions were fluid, shaped by the design, context, and personal habits. Overall, users felt their privacy was often compromised, undervalued, and unprotected. This study advances existing knowledge by emphasizing design's role and offering a synthesized framework capturing the joint influence of perceptual factors on privacy perceptions. It underscores the importance of user experience in privacy evaluations, moving beyond the traditional view of privacy as mere compliance. Moreover, it highlights the paradox of protective mechanisms employing deceptive patterns that compromise user privacy.

Keywords

Cookie consent requests, privacy perceptions, deceptive patterns, deceptive design, privacy by design

1. Introduction

We are facing ever more complex times, when the systems we live by have exceeded our propensity to understand their logic. One of the baffling areas of modern existence pertains to privacy and the paradox of maintaining it in the age of data-driven systems. Media headlines continuously report on data breaches and international legislation, including the General Data Protection Regulation (GDPR) [1] and the ePrivacy Directive [2], raising an alertness to the critical nature of privacy. Under GDPR, it is necessary for users to consent to data collection (i.e., internet cookies) before it occurs [3]. In instances when we have an option to opt-in or opt-out of data sharing, such as when visiting a website, we are shown a message attached to consent options. Yet, these notices are not always designed with the user's best interests in mind [see e.g., 4].

In fact, for decades, web design has included strategies to direct user behavior toward actions that are in the interests of the companies behind the designs and domains, rather than those of the user [5]. This approach to design has many names such as 'deceptive patterns', 'deceptive design', 'manipulative patterns', 'dark patterns', and 'dark design' to name some. These phenomena are visible also in the context of cookie consent requests, which have – more often than not – been seen to include deceptive patterns [6, 7, 8, 9].

This paper contributes to the growing need to understand and protect user privacy while deceptive patterns become increasingly prevalent. Cookie consent requests have an important role in users' ability to control their privacy, yet deceptive patterns have been shown to undermine informed decision-making and diminish user privacy [10, 11, 12]. While cookies can improve a website's functionality and

TKTP 2025: Annual Doctoral Symposium of Computer Science, 2.—3.6.2025 Helsinki, Finland

[*] Corresponding author.

tuokkola.noora@gmail.com (N. Tuokkola); tiina.e.koskelainen@jyu.fi (T. Koskelainen); laura.havinen@uwasa.fi (L. Havinen); rebekah.rousi@uwasa.fi (R. Rousi)
0009-0002-2752-0930 (N. Tuokkola); 0000-0001-9205-4062 (T. Koskelainen); 0009-0000-3364-7407 (L. Havinen); 0000-0001-5771-3528 (R. Rousi)

user experience, unintentionally sharing excess cookie data because of deceptive patterns can impose threats to user privacy [6, 4]. Despite privacy legislation attempting to safeguard user privacy, many organizations still use deceptive design in their services [see e.g., 6, 13].

While prior studies have explored users' emotions and impressions of both deceptive design [e.g., 14, 15, 16] and cookie consent requests [e.g., 17, 18], they often examine them separately, without considering privacy as a holistic user experience. Limited qualitative research [e.g., 19] combines privacy-related factors such as trust, control, risks, and concerns into an integrated view of users' privacy perceptions. Moreover, the influence of deceptive patterns on privacy perceptions remains underexplored [e.g., 20]. This study addresses these gaps by examining privacy as a design-influenced, lived user experience – rather than only a regulatory concern – integrating multiple perceptual factors within a unified qualitative framework.

This study looks at how users perceive privacy in cookie consent requests that feature deceptive patterns and how such design influences their privacy perceptions. The goal is to uncover the influence of unethical design practice on user privacy protection and the complexities of legislatively enforced design mechanisms, in order to encourage improvements to design practices and legislation. Advocating for ethical and transparent design to improve users' privacy perceptions and empower informed choices, the study highlights the crucial role of user experience in privacy research, emphasizing that privacy perceptions are integral in the comprehensive evaluation of a system's privacy. Thus, the main research question is: *What are users' overall perceptions of privacy in cookie consent requests that feature deceptive patterns?* The main question is supported by a subsequent, overarching question of: *What is the role of deceptive patterns in shaping this perception of privacy?*

2. Background and Related Work

Cookies, or the small text files that websites store on users' browsers to track their online interactions [21], serve various purposes, from improving the functionality, security and privacy of the website to making the site more suitable for users' interests [22]. However, not all cookies are essential, and their functionality, origin, and purpose vary, making user consent a critical aspect of data privacy [23], driving policymakers to regulate involuntary data collection.

Legislative changes, such as the GDPR [1] and the ePrivacy Directive [2], now mandate user consent for collecting and using non-essential cookies on any website in the European Union (EU). This is most commonly done by presenting the user with a *cookie consent request* when entering a website. These requests inform users about the purpose, storage, and use of cookies while maintaining informed consent [24]. They also raise users' awareness of their privacy and the company's privacy practices [24]. Under GDPR [1], a cookie consent request must specify what type of data is collected, why, where, and for how long the data will be saved, and whether third parties have access to the cookie data. A good practice would be to not only allow the user to opt-in or opt-out their consent, but to also select which types of cookies they want to provide consent for [24]. Additionally, the request must feature a simple option for rejecting the collection of all non-essential cookies [24], and the user should be able to withdraw their consent as easily as it was given [1]. Crucially, users should be able to access the website even without consenting to non-essential cookies [1].

The topic of cookie consent requests and their impact on user experience continues to be examined in human-computer interaction and information systems research. Many studies observe how the design of cookie consent requests affects user behavior [e.g., 12, 13, 20, 25, 26], meanwhile other studies examine unethical design practices that particularly manipulate users into disclosing more information than they might be comfortable with [e.g., 8, 9, 27, 28, 29].

2.1. Deceptive Patterns in Cookie Consent Requests

Deceptive patterns are design choices that suppress user autonomy by hindering or misleading users from making informed choices [30, 11]. Where these patterns can exist regardless of designers' ill intent [30], they can also be implemented knowingly to reach business aims or even to enable illegal exploitation of user data [4]. One of the first classifications of deceptive patterns has been presented and later updated by Brignull et al. [31], listing 16 different deceptive patterns. In addition, several scholars have presented taxonomies and ontologies of deceptive patterns [see e.g., 32, 33, 30]. Bösch et al. [4] have contributed to the categorization of deceptive patterns by describing strategies that explain the approaches of deceptive patterns in the context of privacy. Also, Soe et al. [9] have suggested additional cookie consent request-specific deceptive pattern types to the existing taxonomies.

Deceptive patterns are frequent in cookie consent requests. For example, Alharbi et al. [6] found deceptive patterns in more than 90 percent of their sample of 100 e-government cookie interfaces and Soe et al. [9] recognized deceptive patterns in 297 of the studied 300 consent notices from news outlet webpages. Following the descriptions by Brignull et al. [31], the typical deceptive patterns in cookie consent requests (based on [6, 34, 8, 35, 36, 9]) are *obstruction; comparison prevention; sneak into basket; visual interference; misdirection; forced action; preselection; nagging*; and *confirmshaming*. These are later exemplified in the mock-ups for this study's user testing.

The GDPR [1], Unfair Commercial Practices Directive (UCPD) [37], and Digital Markets Act (DMA) [38] discourage the use of deceptive patterns in the EU. The UCPD and the DMA prohibit unfair, misleading, and aggressive commercial practices. Additionally, the DMA mandates companies to share important information that consumers need to make well-informed decisions, which deceptive patterns often disguise. Furthermore, the UCPD prohibits companies from hiding or obscuring information in any way that could mislead customers. According to the GDPR, hiding information needed for users' informed consent is prohibited, consent must 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 acceptable.

2.2. Privacy and Online Data Collection

In this study, *privacy* is seen as the protection of an individual and their property. It includes three main perspectives based on previous research [6, 39, 40, 41, 42, 43]: a) an individual should have the right and consent over their own information, b) an individual's information should be concealed from third parties, and c) the solitude of the individual should be preserved.

Online data collection involves various types of information of individuals, such as anonymous, personally unidentifiable, and personally identifiable information [44]. However, not all this data might necessarily be considered private by a person, as privacy perceptions and the desired level of privacy vary [45]. As online data collection has increased, so have individuals' online privacy concerns [46]. This increase has also made individuals more aware and interested in privacy-related questions [47].

Growing concerns and the rise of data collection technologies, such as cookies, has pushed policymakers to regulate online data collection more precisely [1, 2]. In response to the rising risks and concerns that an online environment opposes to privacy, various privacy protection tools have as well emerged [see e.g., 48]. One of the measures to protect user privacy is through design, such as adhering to the Privacy by Design (PbD) principles [49] or taking into account the Privacy Attributes [47] in the user interface design process.

2.3. Related Work on Users' Perceptions of Privacy in Cookie Consent Requests and Deceptive Patterns

Previous research shows that deceptive patterns and poor usability in cookie consent requests primarily have a negative influence on users' privacy perceptions. To outline some key findings, Gray et al. [50] and Mathur et al. [11] found that deceptive patterns undermine and diminish users' sense of privacy. Habib et al. [8] linked deceptive patterns to privacy fatigue caused by frequently encountering consent requests.

Understanding how deceptive patterns influence privacy perceptions begins with users' initial impressions and emotions. Throughout previous studies, users have described deceptive patterns negatively as sneaky, hidden, triggering, forcing, dishonest, unethical, and manipulative [16]. Furthermore, these patterns have been described as ridiculous [14], aggressive, unprofessional, twisted, and short-sighted [50]. Reported emotions include anger, anxiety, annoyance, irritation, frustration, worry, stress, and feeling stupid or pressured [16, 14, 51]. Gray et al. [50] additionally found users feeling distressed, upset, and hostile, as well as some of the following emotions: being nervous, afraid, scared, or jittery. While most studies highlight negative reactions [11], Keleher et al. [52] found the majority of the users in their study to describe interfaces with deceptive patterns with positive adjectives (e.g., honest and ethical), although they still labeled them as intrusive.

Interestingly, some participants in Maier and Harr's [16] study displayed a "resigned" attitude to deceptive patterns, due to excess exposure to the phenomena. Seberger et al. [53] refer to this effect as "resigned acceptance" in which, regardless of whether individuals are bothered by potential privacy breach, they accept it with the acknowledgment that the situation cannot be changed. Similarly, Di Geronimo et al. [15] and Lupiáñez-Villanueva et al. [51] found that the ubiquity of deceptive patterns normalizes them, making users less aware of their negative effects.

2.3.1. Perceptions of Privacy Concerns

Alharbi et al. [6] have stated that privacy is one of the greatest worries of users since websites started using cookies, with the main concern of users being that of who has access to their data. Gray et al. [50] instead found that users' main privacy concerns relate to the type and amount of collected data, as well as fears of unauthorized use for the organization's benefit. The participants of a study by Bongard-Blanchy et al. [14] were concerned about the potential risks that deceptive design could cause, although the participants stated that they were not generally worried about their privacy in relation to deceptive design. Mildner and Savino [54] observed in their study that deceptive patterns caused privacy concerns, leading users to share less data. Lastly, a study by Ha et al. [17] shows that users were concerned about the amount of effort needed for managing the cookie data collection.

2.3.2. Perceptions of Control

Deceptive patterns affect users' control as suppressing user autonomy is at the core of deceptive patterns [11, 55]. Accordingly, Maier and Harr [16] found that users protect their privacy by staying cautious online and recognizing that not all parties act in users' best interest. Graßl et al. [26] have suggested that some deceptive pattern styles could decrease users' perception of control to make informed choices, but more evidence was needed to prove this. A study by Gray et al. [50] showed that users found deceptive patterns to guide them toward certain consent choices in forcing and aggressive ways, which could further translate to reduced control. Furthermore, Lupiáñez-Villanueva et al. [51] found users to perceive interfaces with deceptive patterns as more difficult to understand, less transparent, and unclear regarding the completion of intended actions. Similarly, Gray et al. [50] found participants to describe deceptive patterns as misleading, complicated, and difficult. Additionally, deceptive patterns have been found to cause feelings of powerlessness [56] and a sense of reduced control [54]. Some deceptive patterns create an illusion of control by restricting users' ability to decline consent and instead providing ineffective cookie settings [3, 57, 26]. It should also be noted that some requests may falsely indicate control by registering positive consent when users have declined it [58, 9]. Furthermore, despite regulation, the information in these notices and requests may not be true or accurate [see e.g., 59].

2.3.3. Perceptions of Trust

User's consent choice is largely impacted by their trust in the website [11, 13], while deceptive design erodes trust in websites that use it [60, 51]. This distrust may stem from users perceiving such organizations as dishonest [16]. Mejtoft et al. [20] found that deceptive patterns increase suspicions about a website's trustworthiness and credibility, aligning with Gray et al. [50], where participants described deceptive design as uncanny and inaccurate. Interestingly, while Mejtoft et al. [20] linked cookie acceptance with increased trust, they noted that deceptive design influences consent choices more than trust itself. Conversely, some users in Gray et al. [50] felt sympathy toward data collectors, assuming deceptive patterns were not used on purpose.

2.3.4. Perceptions of Privacy Risks

Users have perceived deceptive patterns as posing risks, such as becoming a crime victim (via e.g., fraud, virus, or hacking) [14, 50]; being lured to buy more resulting in financial loss [14, 11], and losing self-confidence due to more difficult decision-making [14]. Ha et al. reported that while users recognize privacy risks related to cookies, they often take no action [17], possibly due to unawareness of cookies' purpose and function [61, 62]. Moreover, users struggle to assess privacy risks of cookies accurately, as cookie data collection methods may obscure their true extent [61, 62]. Another reason for irrational responses to perceived risks may be that users rely more on intuition rather than rational thinking in consent-giving situations [26, 12]. For instance, they may perceive privacy as easier to relinquish than time and money [e.g., 63], increasing potential privacy risks. Regarding risk-benefit assessments, Maier and Harr [16] found that deceptive design primarily benefits organizations, yet users continue using such services, suggesting the perceived benefits outweigh the risks. Similarly, Gray et al. [50] observed that users view deceptive data collection as self-serving, leading to feelings of undervaluation.

3. Analytical Framework for Perception of Privacy

To guide the qualitative analysis of users' privacy perceptions, an analytical framework for understanding users' perceptions of privacy was constructed by adapting and synthesizing existing models by Adams [19], Chang et al. [64], and Dinev et al. [65]. Adams' [19] model consists of three factors – sensitivity of personal data, trust in the data collector, and the risk-benefit assessment of data usage – culminating in the user's perceived privacy. The model by Chang et al. [64] focuses on how individuals evaluate institutional privacy policies and practices, balancing the perceived security of their personal data with trust and assurance in data handling. The model explores how individuals come to a decision of their privacy boundaries (perceived privacy) – what information to keep private and what to disclose – with factors such as control, risks, concerns, and trust influencing the decision. Dinev et al. [65] describe perceived privacy as an individual's privacy attitude, shaped by perceived control over privacy and privacy risks.

The current framework is not intended as a new theory, but rather as a conceptual lens through which qualitative data on users' privacy perceptions can be interpreted. It adopts elements from each of the three models and is structured around four factors: privacy concerns, control over privacy, trust in the cookie data collector, and perceived privacy risks. Each of these factors influence a user's overall perception of privacy (see Figure 1). Despite previous models focusing on users' perceptions regarding the four influencing factors individually, none has qualitatively looked at how these factors jointly contribute to the overall user experience (perception) of privacy, and what kind of role (deceptive) design has in shaping the perception.

While the previous previous models [19, 64, 65] have studied perceived privacy, the current study distinguishes between *perceived privacy* – a measurable, rational, and often static concept – and the *perception of privacy* – a fluid, subjective, and lived user experience. The current framework attempts to take a qualitative, flexible, interpretive, and user experience-oriented perspective on the topic, in contrast to the quantitative focus on user behavior of the previous models by Chang et al. [64] and Dinev et al. [65]. Adams' [19] model, despite its qualitative applicability, was too narrow on its own to capture comprehensive perceptions. To capture multifaceted perceptions, we consider the individual's thoughts, understandings, feelings, impressions, responses, and beliefs about the state of their privacy.

3.1. The Framework Explained

The theory-informed analytical framework was operationalized across the entire study. Its four factors served as guiding themes shaping the interview themes, guiding the analytical process, and presenting

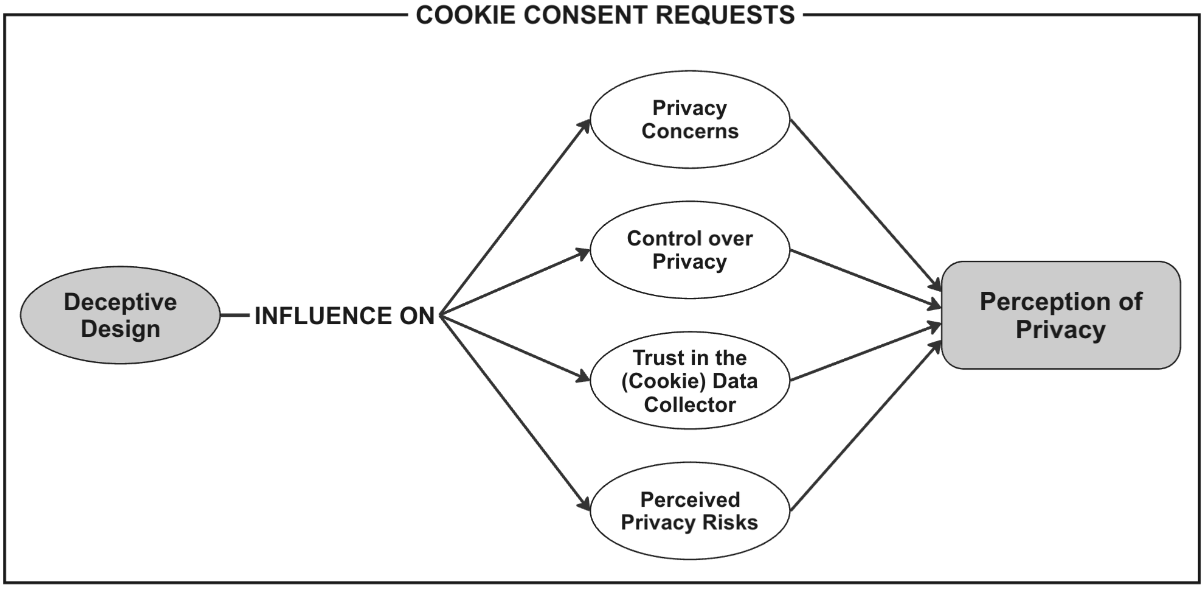


Figure 1: Analytical Framework for the Perception of Privacy

the findings. Relevant theories and models informed the factors' measurement, as detailed next.

Privacy concerns are user anxiety regarding the collection, control, storage, and sharing of personal information [66, 67]. These concerns are initially shaped by an individual's perception of the organization's privacy practices and coherence to them [68]. Westin's privacy concern index [69] and the Concern for Information Privacy (CFIP) [66] model measure these concerns through categories such as threats to personal privacy; collection of excessive personal data; invasion of personal privacy; control over privacy; unauthorized secondary use; improper access; and errors. The scale for Internet Users' Information Privacy Concerns (IUIPC) [67] later refines the CFIP model, focusing on collection, control, and awareness of information privacy practices.

Control is the user's perception of their ability to manage their personal information [68], such as giving consent for cookies. The Communication Privacy Management model [70] focuses on how individuals manage their privacy boundaries – creating a border between private and public information – based on a set of rules [70]. Furthermore, Dinev et al. [65] introduce three aspects of perceived information control: anonymity, secrecy, and confidentiality. Fair Information Practice Principles [71] further influence perceived control over privacy boundaries through ethical guidelines for notice, choice, access, security, and enforcement – helping in understanding data collector adherence to ethical and responsible data collection.

Trust can be defined through its multiple layers. Mayer et al. [72] define organizational trust through three key attributes: the trustee's ability and responsibility, good intentions, and adherence to privacy policies. McKnight et al. [73] extend this to web environments through the following constructs: general willingness to trust; belief that the overall web environment is trustworthy, functional, and secure; belief that the trustee adheres to the legislation and that technology functions reliably; perceived trustworthiness of the trustee; and willingness to depend on the trustee. Gefen and Straub [74] take the definition of trust to digital environments, adding a component of predictability, where trust reduces the uncertainty about the trustee's reliable behavior.

Privacy risks include two different types [75, 76]: behavioral risks – disclosing private information that can be detrimental economically, personally, or sales-wise; and environmental risks – economic risks and privacy risks such as theft of private information or illegal disclosure. A privacy calculus theory has previously been used to explain the influence of risks on perceived privacy [19, 64, 65]. The theory explains how users weigh potential risks against benefits in data-sharing decisions, which in digital environments is influenced by privacy concerns regarding third-party data sharing; trust in the data collector; perceived reliability of the data exchange situation; and personal motivation for sharing the information [75]. Privacy calculus can additionally explain users' disposition to valuing their privacy.

A design factor was added to the framework to examine how deceptive patterns influence privacy perceptions, as existing research suggests a potential connection between design and privacy perceptions, although it has not been definitively established. For example, the Online Buying Persuasion model (OBP) [77] shows that a website's design affects customer satisfaction, which in turn affects trust. As shown in the models by Chang et al. [64] and Adams [19], trust directly affects perceived privacy. Similar to the OBP model, a study by Lai [78] shows that design affects the system's perceived usefulness and perceived ease of use (also applying to the usability of privacy protection mechanisms), which influence motivation to use. Additionally, Bélanger and Crossler [79] found that design choices, such as transparency, could influence users' trust and privacy concerns. Lastly, multiple scholars [e.g., 49, 47] have discovered a relationship between design and user privacy, leading to the need to develop privacy-protective design guidelines.

4. Methodology

In this study, a qualitative approach was taken, combining user testing, think-aloud, and thematic interviews to capture users' multifaceted privacy perceptions in relation to deceptive patterns in cookie consent requests. This triangulated approach was chosen for its ability to reveal nuanced insights into user behavior, attitudes, and experiences [80, 81, 82]. The study was conducted online via Microsoft Teams in compliance with the Finnish Code of Conduct for Research Integrity [83] and GDPR [1].

Participants were informed about the study's purpose, procedures and any potential risks or benefits. They received an information leaflet and a privacy notice via email prior to the study, and informed consent was obtained before participation. The study was voluntary for participants and they had the right to withdraw at any point. External ethical clearance was not required, as the study involved only adults, did not include vulnerable populations, and did not collect personal, invasive, or medical data [84]. Data was handled anonymously and transcriptions followed the participants' answers verbatim, with only bodily expressions and sighs left out.

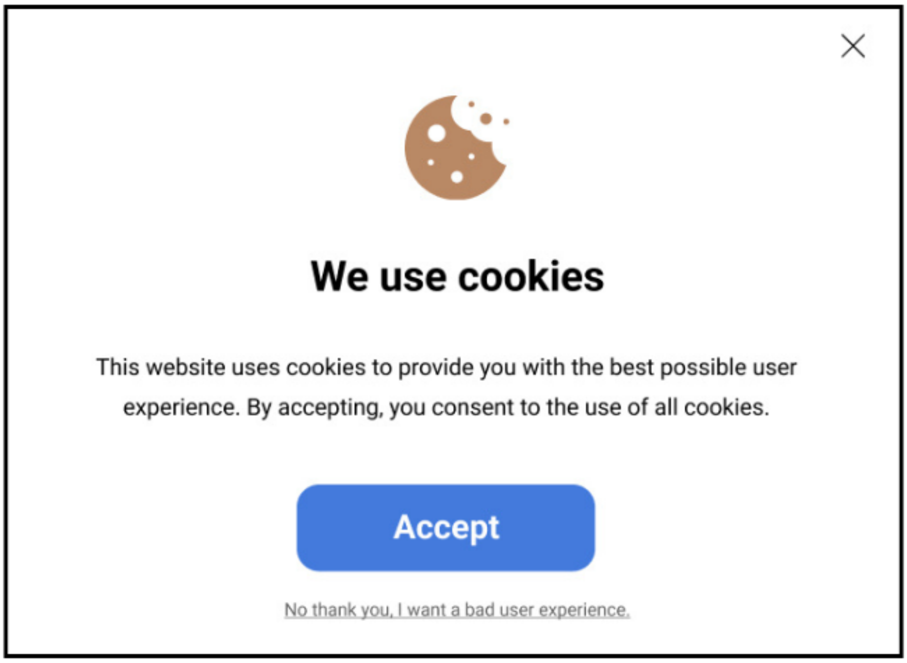
The participants (N=8) selected for the study were Generation Z university students, born between 1995 and 2002. The gender representation was five females, two males, and one other. Seven interviews were conducted in Finnish and one in English. The participants were bachelor's (five) and master's (three) level students, representing various academic fields: information technology, humanities, arts, education, health and well-being, natural sciences, and economics.

4.1. User Testing and Think-Aloud Protocol

User testing was conducted with three high-fidelity cookie consent request mock-ups. The participants had a simple task of opting in or out of cookie data collection in order to proceed to the website. Concurrently with the user testing, the participants were encouraged to verbalize their thoughts and feelings while interacting with the interface.

Three mock-ups were designed in Figma, containing the most common cookie consent request styles [e.g., 85, 6, 23] and the most common deceptive patterns found in cookie consent requests [e.g., 6, 34, 8, 35, 36, 9]. Figure 2 presents the first mock-up as an example[1]. The first mock-up is a binary choice between accepting or declining cookies, with a short text explaining the practical information related to cookie data collection. Four deceptive patterns were intentionally used in this mock-up. *Misdirection* shifted the user's focus from the decline-button to the big and colorful accept-button, *visual interference* disguised the decline button as unimportant text, *forced action* made the user return to the request to make a consent choice if they tried to close it by clicking the X, and *confirmshaming* made the text of the decline-option emotionally manipulative in trying to get the user to steer away from it (i.e., "bad user experience").

[1] The figures of all three mock-ups are accessible at https://doi.org/10.6084/m9.figshare.29118059



We use cookies

This website uses cookies to provide you with the best possible user experience. By accepting, you consent to the use of all cookies.

Figure 2: The first mock-up

The second mock-up is an informational cookie interface. This mock-up has more text and an option to read more about the privacy policy and cookie data collection. The consent options in this mock-up were to accept all cookies or go to settings where different types of cookies could be selected from. This mock-up consisted of at least five deceptive pattern types. *Misdirection* was used similarly to the first mock-up; *visual interference* disguised the decline-option as a settings-button and did not specify what settings it directs to; *forced action* made it seem like declining all cookie types would be possible when in reality essential cookies were mandatory to accept; *nagging* appeared in the error message of attempting to decline essential cookies by requesting the user to accept them, which is not in their best interest; and *confirmshaming* made accepting all cookies seem more beneficial than declining them.

The style of the third mock-up is called cookie categories (also known as multiple-choice banner or numerous options banner). The categories could be selected with radio buttons and the consent options were ”accept all” and ”save settings”. Three deceptive patterns were intentionally added to this mock-up: *preselection* introduced all cookie types as preselected options; *comparison prevention* presented the user with many options in a complex manner making it more difficult to compare cookie types for making a consent choice; and *misdirection* showed an imbalance between accepting all cookies and saving settings.

The second and third mock-ups did not include a simple option to decline consent. Additionally, they included a deceptive pattern called *sneak into basket*, guiding the user toward accepting all cookies instead of saving their selected cookie category settings. This pattern sneaks both non-essential and essential cookies in the data collection, as the user may mistakenly click ”accept all” even if they intended to consent to fewer cookie categories. All of the mock-ups blocked access to the website before making the consent choice, which was intentionally done so that the participant would have to complete the request and think about its design. Blocking access to the website before consenting to cookies is a type of deceptive pattern called *obstruction*.

4.2. Semi-Structured Thematic Interviews

Following the user testing, semi-structured thematic interviews were conducted to gain deeper insights into participants’ experiences, impressions, attitudes, beliefs, and perceptions of privacy regarding each of the four influencing factors from the analytical framework. Semi-structured interview method was chosen due to its flexibility, as it allows for discussing specific themes while encouraging participant-led, open-ended responses that genuinely reflect the participant's perceptions.

4.3. Data Overview and Analysis

The study sessions, each lasting between 90-130 minutes, produced 513 pages of transcribed data, offering rich qualitative insights on the topic. Although the study employed three different data collection methods, they were conducted as a single, continuous session per participant, resulting in integrated, continuous discussions that were transcribed and analyzed as unified datasets rather than separated by method, with all parts contributing equally to the findings.

The data analysis followed a qualitative content analysis approach [86], supported by the structural steps of thematic analysis [87]. First, coding, theme development, and refinement were conducted iteratively, guided by the analytical framework. Then, the coded data was organized using Excel, where themes were further synthesized into broader categories. Repetitive responses were also quantified to highlight the prevalence of key patterns. The elements of thematic analysis were used to help organize the data, but the overall analysis and interpretation were primarily rooted in content analysis. The structured themes and categories served as a foundation for the study's findings.

5. Results

The results are presented in four sections, following the factors from the analytical framework. Lastly, additional findings influencing the overall privacy perceptions in the context of cookie consent requests are presented.

5.1. Privacy Perceptions in Relation to Concerns

Just over half of the participants (5/8) perceived deceptive patterns to increase their privacy concerns. Many described deceptive cookie consent requests as dishonest, unclear, and difficult to understand, which heightened suspicion of the data collector's intentions. Similarly, the motives behind deceptive data collection were questioned:

> *It just makes me feel uncertain about what my information is actually used for because they are so difficult to understand.* (P6)

> *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.* (P3)

In contrast, the rest of the participants (3/8) did not find deceptive patterns to meaningfully increase their privacy concerns. Some already had high online privacy concerns, while others consciously avoided thinking about privacy concerns to avoid frustration or anxiety:

> *I try to keep my sanity by thinking that [sharing my data] can't be that bad... maybe it's just easier to not think about it.* (P2)

For some, perceived control over privacy choices mitigated concerns. P4, for instance, said that deceptive design did not meaningfully affect their concerns, as they felt capable managing their consent choice. While P1 saw deceptive patterns as a reminder to stay in control rather than as threats to privacy.

Overall, while deceptive patterns heightened privacy concerns for some, most participants felt the increase was not substantial enough to negatively influence their overall sense of privacy: "*[Deceptive design] increases my suspicion and worrying... but ultimately, not enough*" (P7).

5.2. Privacy Perceptions in Relation to Control

Most participants (7/8) perceived that deceptive design either decreased their ability to control their privacy or made controlling more difficult. While many acknowledged that control has a substantial positive influence on their privacy, they believed that deceptive patterns (e.g., comparison prevention or misdirection) mainly add obstacles rather than entirely diminish control. Regardless, some participants still felt in control, shaping their overall perception of privacy:

> *If I feel that I can control the things related to my privacy, then yes, I think that my privacy is in a better state.* (P5)

For some other participants, deceptive design was a major barrier to their privacy, making them frustrated and even anxious due to the perceived loss of autonomy, for example:

> *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.* (P8)

In contrast, one participant initially claimed deceptive patterns to only have little influence on their privacy perception due to being accustomed to encountering them in cookie consent requests, but later acknowledged that some patterns could create obstacles to managing their privacy:

> *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.* (P7)

Many participants (such as P3, P4, P5, and P6) agreed that the influence of deceptive design depended on the specific patterns used:

> *I think [my perception] varies a lot. There are so many different [deceptive patterns].* (P4)

Five participants felt that the persuasive and manipulative nature of deceptive patterns deliberately guided them toward accepting all cookies, making declining cookies feel less like an autonomous, informed, and voluntary choice:

> *[Deceptive patterns] try to persuade or guide me toward accepting all... That option looks much more tempting to click on.* (P5)

Beyond influencing choices, deceptive patterns often made the requests unclear, uninformative, unpredictable, and difficult to understand (expressed by 5/8 participants). Some struggled to find essential information, which made navigating the request more complicated, requiring additional effort to maintain control over one's consent choice:

> *It's a lot of work to figure out... Sometimes it's designed in a very difficult way, like a piece of code to me [a non-programmer], and I have to read through it very carefully.* (P2)

These barriers resulted in exclusively negative emotions, such as annoyance, frustration, and even anger (indicated by 7/8 participants), as deceptive patterns were perceived as obstructive and time-consuming:

> *It makes me angry. It frustrates me because I just wanna complete [the request] as effortlessly as possible.* (P4)

5.3. Privacy Perceptions in Relation to Trust

Almost all participants (7/8) reported lower trust in the cookie data collector when deceptive design was used, negatively influencing their privacy perceptions. Deceptive patterns in the cookie consent requests made the collector seem dishonest and raised suspicions about data usage:

> *If they use deceptive design, and they are not capable of doing it in an honest way, it doesn't inspire trust in me.* (P6)

The lack of transparency and care for users' interests made the participants skeptical, cautious and uneasy about what happens to their personal data:

> *I can't immediately find the information about what my cookie data is used for... so maybe there could be something else going on that is not told.* (P2)

Deceptive patterns also indicated a lack of ethical responsibility, eroding the participants' trust. While some described a gradual decline in trust, others experienced a complete loss:

> *It shakes my trust every time I see them use a deceptive tactic. The more I encounter deceptive design... my trust just starts crumbling down and diminishing.* (P1)

One participant's trust, however, remained unaffected: ”*I want to trust them because it's also for their own benefit to be truthful and trustworthy*” (P4).

Some participants perceived that deceptive patterns in the cookie consent request make it seem like the data collector is prioritizing its own interests over the user's privacy. Furthermore, no participant found deceptive patterns to offer any personal benefit – instead, five participants believed deceptive design solely existed for the collector's financial and operational advantage:

> *[The cookie data collectors], for sure, do not think what is best for the user, they just think what is best for them.* (P3)

> *It seems that [the cookie data collectors] are desperate to gather as much data as possible... not for my benefit, but for their own.* (P6)

Approximately six participants perceived deceptive design as evidence of the cookie data collector's incompetence, non-benevolence, unpredictability, and dishonesty, making the collector seem untrustworthy:

> *I kind of feel like [the data collectors] treat me in a degrading way.* (P2)

> *If it's designed deceptively, it makes me question whether [the collectors] are honest.* (P1)

> *[Deceptive design] projects a certain lack of professionalism... it doesn't feel like the request was designed by a professional.* (P8)

Despite the dominant perception of decreased trust, some participants empathized with the data collectors, expressing a desire to trust them and speculating that they might not be intentionally using deceptive patterns to harm the users:

> *I don't want to think bad about them because they are ”just doing their job”. They might not be [using deceptive design] on purpose.* (P8)

5.4. Privacy Perceptions in Relation to Risks

Half of the participants (4/8) believed that deceptive design increased privacy risks, primarily due to uncertainty about what the cookie data is used for and with whom it is shared:

> *Yeah, deceptive design does increase the feeling of risks... I am not sure what the information is being used for or my information might be used wrongly.* (P5)

In addition to this uncertainty, six participants described deceptive patterns making the consent requests more difficult to understand, amplifying mistrust and further heightening perceived privacy risks:

> *It's often unclear what my data is used for. And do I then trust that the information is only used for what I give permission for? Maybe they just are so difficult to understand and trust in the first place.* (P6)

For these participants, the greatest risk that deceptive design could cause was the potential misuse or illegal use of cookie data. A more frequently discussed risk was accidentally or unknowingly sharing more cookie data than intended due to deceptive patterns:

> *Deceptive patterns might make me click on something that I don't wanna click and then I might share more information than I intended or my information may be shared with people that I don't wanna share with.* (P7)

The suspiciousness of unclear or misleading consent requests contributed to a heightened sense of privacy risks:

> *If the request is not straightforward and circles around any other option than accepting all... It makes me think that there's something they are trying to hide, making me think there are more risks involved.* (P3)

While most participants reported an increase in perceived privacy risks, three stated that deceptive design doesn't have a direct connection with actual privacy risks:

> *My idea of risks doesn't get triggered by how the cookie banner is designed.* (P7)

Only one participant reported deceptive design to decrease perceived privacy risks, as it simplifies decision-making:

> *Deceptive design makes it clearer and easier to make the [accept all] choice, so I don't see any risks of choosing wrong.* (P8)

Despite this, most participants (7/8) weighed the potential benefits of cookies against the perceived privacy risks when making a consent choice, sometimes leading to avoiding websites that excessively use deceptive patterns.

5.5. Additional Findings

The participants' privacy perceptions were influenced by personal interest, the ubiquity of cookie consent requests and deceptive design, and reluctance to think about privacy. Most participants (6/8) commented that their personal interest toward privacy and thus, their own active control over their privacy, is a more meaningful factor for their perception of privacy than deceptive design. Furthermore, five participants perceived deceptive design to be a common part of their internet use, with some being used to actively avoiding the misleading and deceptive consent options. Additionally, five participants noted that cookie consent requests are so common that they barely notice them when browsing the web, making it difficult to describe how they feel about their privacy as it feels less significant. Lastly, three participants expressed privacy to be a difficult or even intimidating topic, leading to reluctance to think about it.

6. Discussion

This chapter discusses participants' impressions and attitudes toward deceptive design in cookie consent requests, reflecting how such design influences their perceptions of privacy as protected, respected, compromised, undervalued, or unimpacted.

6.1. Control over Privacy

The results point out that deceptive patterns contribute to a general loss of perceived control over user privacy. This is potentially caused by the feeling of being undervalued due to data collector non-benevolence, and impressions of manipulation. This finding is supported by Gray et al. [50], who found that the use of deceptive patterns prioritizes organizational interests and pressures users in forceful and aggressive ways toward certain consent choices. Participants in the current study also described deceptive cookie consent requests as complicated, unclear, and difficult to understand, further diminishing perceived control and potentially disempowering informed consent choices. These perceptions of diminished control contribute to a perception of user privacy being undervalued or compromised when deceptive design is used.

Additionally, participants often chose to ignore potential issues related to deceptive design despite recognizing them. Ignoring or minimizing the existing privacy issues could imply that consciously interacting and constantly being worried about them would require more cognitive effort than the users would be willing to invest in their interaction with cookie consent requests.

6.2. Trust and Transparency Issues

Deceptive design seemed to diminish participants' trust in cookie data collectors, mainly due to a lack of transparency and perceived dishonesty. These findings are consistent with previous studies [16, 51, 20, 60]. Distrust and lack of transparency may be taken to indicate that the users perceive their privacy to be at risk, as the findings are contrary to privacy-protective design principles [49, 47]. Keleher et al. [52] found users to perceive interfaces with deceptive design more positively – describing them as honest and ethical, coercing users to make the ”right” decisions – suggesting that researchers often wrongly assume users' perceptions. The overall negative findings of the current and previous research challenge the argument made by Keleher et al. [52].

However, similar to Gray et al. [50], some participants expressed empathy toward the cookie data collector, highlighting the complexity of users' perceptions: while they might not trust the data collector, they recognize that not all of them consciously act maliciously. Despite empathy, the general lack of trust caused by deceptive design suggests an overall perception of privacy not being well protected.

6.3. Privacy Concerns and Risks

Consistent with the privacy calculus theory, participants often weighed benefits against perceived risks, leading them to compromise their privacy for convenience. Users may be aware of the risks but their perception of the severity of those risks is downplayed by the immediate benefits. This suggests a more pragmatic viewpoint on privacy, aligning with existing research that has shown users to often rely on intuitive judgments rather than rational analysis in consent-giving situations [26, 12]. This highlights the tension between users' awareness of privacy risks and their perception of trade-offs, further emphasizing the complexity of privacy perceptions in the digital environment.

One finding in this study was related to users' habitual engagement due to deceptive design and cookie consent requests' ubiquity and general reluctance to think about privacy concerns and risks. This aligns with Maier and Harr [16] and Seberger et al. [53] who suggest that users have a resigned attitude toward privacy issues due to deceptive design's prevalence in daily life. The resignation 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 issues may stop users from critically evaluating cookie consent requests, as suggested by Lupiáñez-Villanueva et al. [51].

6.4. Users' Descriptions and Reactions to Deceptive Cookie Consent Requests

Participants predominantly expressed negative emotions such as frustration, annoyance, and uncertainty towards deceptive cookie consent requests, leading them to doubt the cookie data collector's privacy measures and intentions. Compared to previous studies, uncertainty was a pronounced feeling in this study. 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. Furthermore, deceptive design was described as suspicious and misleading, reflecting mistrust in cookie consent requests and cookie data collectors.

Building on previous studies' characterizations of cookie data collectors, participants in this study described them as non-benevolent, dishonest, and even incapable. Mayer et al. [72] argue that benevolence and capability are crucial building blocks for trust. From this perspective, the findings of the current study suggest that deceptive patterns in cookie consent requests increase uncertainty, thereby diminishing users' trust. Overall, the prevalence of these negative characterizations further suggest that users generally perceive their privacy as neither respected nor protected.

7. Conclusion

This study explored how users perceive privacy in cookie consent requests featuring deceptive patterns, and how such design practices shape these perceptions. By combining user testing, a think-aloud protocol, and thematic interviews, multifaceted perceptions were captured. The findings suggest that privacy is not perceived binarily as negative or positive, protected or compromised, but rather as a flexible concept shaped by specific deceptive patterns, habitual behaviors, and personal interest in privacy protection. However, deceptive patterns predominantly influenced these perceptions negatively, leading users to perceive their privacy as compromised, undervalued, and unprotected. The overall negative perceptions stemmed from feelings of frustration, mistrust, uncertainty, and lack of control, as well as skepticism toward deceptive design. Although users may have learned to withstand or bypass deceptive patterns, they still perceive them as undermining user privacy, suggesting it is neither fully protected nor respected.

An analytical framework was developed by adapting prior models, structured around four key factors influencing privacy perceptions: privacy concerns, control over privacy, trust in data collectors, and perceived privacy risks. While these dimensions have been addressed individually in previous research – and many findings align with prior studies – this study contributes by demonstrating their combined influence on users' overall privacy perceptions in the context of deceptive cookie consent requests. It distinguishes itself by integrating these factors into a qualitative, synthesized, and user experience-oriented perspective on privacy. The findings further suggest expanding the framework to include design and emotional factors, as strong emotional responses notably shaped users' perceptions. The framework thus offers a more holistic understanding of privacy especially within legislatively mandated interface designs, providing a conceptual lens for future research investigating users' privacy perceptions in response to evolving interface designs and regulatory environments.

Beyond its theoretical contributions, this study also draws attention to the crucial role of user experience in privacy research. Privacy perceptions are not only central to users' trust in digital services and data collectors, but they also form an essential component for evaluating a system's overall privacy. This challenges the traditional compliance-based approach by showing that privacy should additionally be assessed as a lived, design-mediated experience. On a practical level, the study advocates for treating privacy as a user experience issue, urging designers, developers, and policymakers to adopt privacy-protective, transparent design principles [such as, 49, 47]. Embedding such principles into legislative frameworks could clarify compliance requirements. Societally, this study calls for stricter privacy legislation explicitly prohibiting deceptive design practices, to enhance user trust and autonomy in online interactions.

While the study's limitations include a small sample size (N=8), a specific demographic (generation Z university students), and a limited context (mock-up cookie consent requests), it provides a holistic, user experience-oriented foundation for future research. Future studies should empirically test and refine the analytical framework in diverse, real-world settings. Large-scale quantitative research could complement the qualitative insights, while design-specific research could isolate which deceptive patterns most influence users' perceptions and why, leading to actionable privacy-protective design guidelines.

In conclusion, as deceptive design continues to affect user privacy, this study calls for an industry-wide commitment to ethical, transparent, and user-centric design of protective systems, which would empower users to navigate online services without compromising privacy while enhancing their trust in digital platforms and the parties behind them.

Acknowledgments

We gratefully acknowledge the support of the Faculty of Information Technology at the University of Jyväskylä, as well as the School of Technology and Innovations, and the School of Marketing and Communication at the University of Vaasa. We also thank the Research Council of Finland for its support and funding of the project *Emotional Experience of Privacy and Ethics in Everyday Pervasive Systems* (BUGGED) (decision number 348391).

Declaration on Generative AI

During the preparation of this work, the authors used GPT-4 by ChatGPT in Sections 2, 3, and 6 to improve writing style to enhance readability, check grammar and spelling, and reword sentences to improve clarity. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] European Union, 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, 2016.

[2] European Union, 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, 2002.

[3] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, I. Santos, Can I opt out yet? GDPR and the global illusion of cookie control, in: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Association for Computing Machinery, New York, NY, USA, 2019, pp. 340–351. doi:10.1145/3321705.3329806.

[4] C. Bösch, B. Erb, F. Kargl, H. Kopp, S. Pfattheicher, Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns, in: Proceedings on Privacy Enhancing Technologies, volume 2016, De Gruyter, 2016, pp. 237–254. doi:10.1515/popets-2016-0038.

[5] H. Brignull, Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You, Testimonium Ltd, 2023.

[6] J. A. Alharbi, A. S. Albesher, H. A. Wahsheh, An Empirical Analysis of E-Governments' Cookie Interfaces in 50 Countries, Sustainability 15 (2023) 1231. doi:10.3390/su15021231.

[7] C. Krisam, H. Dietmann, M. Volkamer, O. Kulyk, Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites, in: Proceedings of the 2021 European Symposium on Usable Security, Association for Computing Machinery, New York, NY, USA, 2021, pp. 1–8. doi:10.1145/3481357.3481516.

[8] H. Habib, M. Li, E. Young, L. Cranor, "Okay, whatever": An Evaluation of Cookie Consent Interfaces, in: CHI Conference on Human Factors in Computing Systems, ACM, New Orleans, LA, USA, 2022, pp. 1–27. doi:10.1145/3491102.3501985.

[9] T. H. Soe, O. E. Nordberg, F. Guribye, M. Slavkovik, Circumvention by design - dark patterns in cookie consent for online news outlets, in: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society, ACM, Tallinn, Estonia, 2020, pp. 1–12. doi:10.1145/3419249.3420132.

[10] H. Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. F. Cranor, N. Sadeh, F. Schaub, An empirical analysis of data deletion and Opt-Out choices on 150 websites, in: Fifteenth Symposium on Usable Privacy and Security, USENIX Association, Santa Clara, CA, USA, 2019, pp. 387–406. URL: https://www.usenix.org/conference/soups2019/presentation/habib.

[11] A. Mathur, M. Kshirsagar, J. Mayer, What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA, 2021, pp. 1–18. doi:10.1145/3411764.3445610.

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

[13] M. Nouwens, I. Liccardi, M. Veale, D. Karger, L. Kagal, Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, in: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, Honolulu, HI, USA, 2020, pp. 1–13. doi:10.1145/3313831.3376321.

[14] K. Bongard-Blanchy, A. Rossi, S. Rivas, S. Doublet, V. Koenig, G. Lenzini, "I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - Dark Patterns from the End-User Perspective, in: Proceedings of the 2021 ACM Designing Interactive Systems Conference, Association for Computing Machinery, New York, NY, USA, 2021, pp. 763–776. doi:10.1145/3461778.3462086.

[15] L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, A. Bacchelli, UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception, in: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA, 2020, pp. 1–14. doi:10.1145/3313831.3376600.

[16] M. Maier, R. Harr, Dark Design Patterns: An End-User Perspective, Human Technology 16 (2020) 170–199. doi:10.17011/ht/urn.202008245641.

[17] V. Ha, K. Inkpen, F. Al Shaar, L. Hdeib, An examination of user perception and misconception of internet cookies, in: Extended Abstracts on Human Factors in Computing Systems, ACM, Montréal, Québec, Canada, 2006, pp. 833–838. doi:10.1145/1125451.1125615.

[18] O. Kulyk, A. Hilt, N. Gerber, M. Volkamer, "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer, in: Proceedings of the 3rd European Workshop on Usable Security, Internet Society, London, England, 2018. doi:10.14722/eurousec.2018.23012.

[19] A. Adams, Users' Perception of Privacy in Multimedia Communication, CHI99: Conference on Human Factors in Computing Systems 15-20 May (1999) 53–54. doi:10.1145/632716.632752.

[20] T. Mejtoft, N. Vejbrink Starbrink, C. Roos Morales, O. Norberg, M. Andersson, U. Söderström, Cookies and Trust: Trust in organizations and the design of cookie consent prompts, in: Proceedings of the European Conference on Cognitive Ergonomics 2023, Swansea, UK, 2023, pp. 1–6. doi:10.1145/3605655.3605668.

[21] D. M. Kristol, HTTP Cookies: Standards, privacy, and politics, ACM Transactions on Internet Technology 1 (2001) 151–198. doi:10.1145/502152.50215.

[22] Finnish National Cyber Security Centre - Traficom, Cookies, 2024. URL: https://www.

kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/cookies.

[23] M. Kretschmer, J. Pennekamp, K. Wehrle, Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web, ACM Transactions on the Web 15 (2021) 1–42. doi:10.1145/3466722.

[24] Finnish Transport and Communications Agency - Traficom, Cookies and other data stored on users' terminal devices and the use of such data – Guidelines for service providers, 2022. URL: https://www.traficom.fi/sites/default/files/media/regulation/Guidance_on_the_use_of_web_cookies_for_the_service_providers%20%28002%29.pdf.

[25] C. Bermejo Fernandez, D. Chatzopoulos, D. Papadopoulos, P. Hui, This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices, Proceedings of the ACM on Human-Computer Interaction 5 (2021) Article No. 346. doi:10.1145/3476087.

[26] P. Graßl, H. Schraffenberger, F. Z. Borgesius, M. Buijzen, Dark and bright patterns in cookie consent requests, Journal of Digital Social Research 3 (2021) 1–38. doi:10.33621/jdsr.v3i1.54.

[27] B. M. Berens, H. Dietmann, C. Krisam, O. Kulyk, M. Volkamer, Cookie Disclaimers: Impact of Design and Users' Attitude, Proceedings of the 17th International Conference on Availability, Reliability and Security (2022) Article No. 12. doi:10.1145/3538969.3539008.

[28] G. Kampamos, S. F. Shahandashti, Accept All: The Landscape of Cookie Banners in Greece and the UK, in: ICT Systems Security and Privacy Protection. SEC 2021, volume 625, Springer International Publishing, Cham, 2021, pp. 213–227. doi:10.1007/978-3-030-78120-0_14.

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

[30] C. M. Gray, C. T. Santos, N. Bielova, T. Mildner, An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building, Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (2024) Article No. 289. doi:10.1145/3613904.3642436.

[31] H. Brignull, M. Leiser, C. Santos, K. Doshi, Deceptive patterns – user interfaces designed to trick you, 2023. URL: https://www.deceptive.design/.

[32] G. Conti, E. Sobiesk, Malicious interface design: Exploiting the user, in: Proceedings of the 19th International Conference on World Wide Web, Association for Computing Machinery, New York, NY, USA, 2010, pp. 271–280. doi:10.1145/1772690.1772719.

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

[34] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, A. L. Toombs, The Dark (Patterns) Side of UX Design, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, Montreal, QC, Canada, 2018, pp. 1–14. doi:10.1145/3173574.3174108.

[35] M. Martini, C. Drews, Making Choice Meaningful – Tackling Dark Patterns in Cookie and Consent Banners through European Data Privacy Law, Available at SSRN, 2022. doi:10.2139/ssrn.4257979.

[36] T. Mejtoft, E. Frängsmyr, U. Söderström, O. Norberg, Deceptive Design: Cookie Consent and Manipulative Patterns, in: 34th Bled eConference Digital Support from Crisis to Progressive Change: Conference Proceedings, University of Maribor Press, Online, 2021, pp. 393–404. doi:10.18690/978-961-286-485-9.29.

[37] European Union, 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, 2005.

[38] European Union, 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, 2022.

[39] I. Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Brooks/Cole, Monterey, California, USA, 1975.

[40] R. A. Posner, The Economics of Privacy, The American Economic Review 71 (1981) 405–409.

[41] D. M. Pedersen, Model for Types of Privacy by Privacy Functions, Journal of Environmental Psychology 19 (1999) 397–405. doi:10.1006/jevp.1999.0140.

[42] S. D. Warren, L. D. Brandeis, The Right to Privacy, Harvard Law Review 4 (1890) 193–220.

[43] A. F. Westin, Privacy and Freedom, Athenaeum, New York, USA, 1967.

[44] R. K. Chellappa, R. G. Sin, Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma, Information Technology and Management 6 (2005) 181–202. doi:10.1007/s10799-005-5879-y.

[45] S. Petronio, Communication Privacy Management, The International Encyclopedia of Communication Theory and Philosophy (2016) 1–9. doi:10.1002/9781118766804.wbiect138.

[46] A. I. Antón, J. B. Earp, J. D. Young, How internet users' privacy concerns have evolved since 2002, IEEE Security & Privacy 8 (2010) 21–27. doi:10.1109/MSP.2010.38.

[47] S. Barth, D. Ionita, P. Hartel, Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines, ACM Computing Surveys 55 (2022) 63:1–63:37. doi:10.1145/3502288.

[48] J. Waldo, H. S. Lin, L. I. Millett, Engaging Privacy and Information Technology in a Digital Age: Executive Summary, Journal of Privacy and Confidentiality 2 (2010) 5–18. doi:10.29012/jpc.v2i1.580.

[49] A. Cavoukian, Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D, Identity in the Information Society 3 (2010) 247–251. doi:10.1007/s12394-010-0062-y.

[50] C. M. Gray, J. Chen, S. S. Chivukula, L. Qu, End User Accounts of Dark Patterns as Felt Manipulation, Proceedings of the ACM on Human-Computer Interaction 5 (2021) 372:1–372:25. doi:10.1145/3479516.

[51] F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation : Final Report, Technical Report, Publications Office of the European Union, 2022. URL: https://data.europa.eu/doi/10.2838/859030.

[52] M. Keleher, F. Westin, P. Nagabandi, S. Chiasson, How Well Do Experts Understand End-Users' Perceptions of Manipulative Patterns?, in: Nordic Human-Computer Interaction Conference, Association for Computing Machinery, New York, NY, USA, 2022, pp. 1–21. doi:10.1145/3546155.3546656.

[53] J. S. Seberger, M. Llavore, N. N. Wyant, I. Shklovski, S. Patil, Empowering resignation: There's an app for that, Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (2021) Article No. 552. doi:10.1145/3411764.3445293.

[54] T. Mildner, G.-L. Savino, Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook, Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (2021) Article No. 464. doi:10.1145/3411763.3451659.

[55] T. Kollmer, A. Eckhardt, Dark Patterns: Conceptualization and Future Research Directions, Business & Information Systems Engineering 65 (2023) 201–208. doi:10.1007/s12599-022-00783-7.

[56] L. Sánchez Chamorro, R. Toebosch, C. Lallemand, Manipulative Design and Older Adults: Co-Creating Magic Machines to Understand Experiences of Online Manipulation, in: Proceedings of the 2024 ACM Designing Interactive Systems Conference, Association for Computing Machinery, New York, NY, USA, 2024, pp. 668 – 684. doi:10.1145/3643834.3661513.

[57] Forbrukerrådet, Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Rights to Privacy, Report, 2018. URL: https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf.

[58] C. Matte, N. Bielova, C. Santos, Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework, in: 2020 IEEE Symposium on Security and Privacy, IEEE, San Francisco, CA, USA, 2020, pp. 791–809. doi:10.1109/SP40000.2020.00076.

[59] J.-R. Piispanen, T. Myllyviita, V. Vakkuri, R. Rousi, Smoke screens and scapegoats: The reality of general data protection regulation compliance – privacy and ethics in the case of replika ai, 2024.

arXiv:2411.04490.

[60] A. M. Bhoot, M. A. Shinde, W. P. Mishra, Towards the Identification of Dark Patterns: An Analysis Based on End-User Reactions, in: Proceedings of the 11th Indian Conference on Human-Computer Interaction, Association for Computing Machinery, New York, NY, USA, 2020, pp. 24–33. doi:10.1145/3429290.3429293.

[61] R. Beckwith, Designing for ubiquity: the perception of privacy, IEEE Pervasive Computing 2 (2003) 40–46. doi:10.1109/MPRV.2003.1203752.

[62] S. Flinn, J. Lumsden, User Perceptions of Privacy and Security on the Web, Report, National Research Council Canada, 2005.

[63] L. Sánchez Chamorro, C. Lallemand, C. M. Gray, "My Mother Told Me These Things are Always Fake"—Understanding Teenagers' Experiences with Manipulative Designs, in: Proceedings of the 2024 ACM Designing Interactive Systems Conference, Association for Computing Machinery, New York, NY, USA, 2024, pp. 1469–1482. doi:10.1145/3643834.3660704.

[64] Y. Chang, S. F. Wong, C. F. Libaque-Saenz, H. Lee, The role of privacy policy on consumers' perceived privacy, Government Information Quarterly 35 (2018) 445–459. doi:10.1016/j.giq.2018.04.002.

[65] T. Dinev, H. Xu, J. H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, European Journal of Information Systems 22 (2013) 295–316. doi:10.1057/ejis.2012.23.

[66] H. J. Smith, S. J. Milberg, S. J. Burke, Information Privacy: Measuring Individuals' Concerns about Organizational Practices, MIS Quarterly 20 (1996) 167. doi:10.2307/249477.

[67] N. K. Malhotra, S. S. Kim, J. Agarwal, Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, Information Systems Research 15 (2004) 336–355. doi:10.1287/isre.1040.0032.

[68] H. Xu, T. Dinev, J. Smith, P. Hart, Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances, Journal of the Association for Information Systems 12 (2011) 798–824. doi:10.17705/1jais.00281.

[69] P. Kumaraguru, L. F. Cranor, Privacy Indexes: A Survey of Westin's Studies, Technical Report, Institute for Software Research International, Carnegie Mellon University, 2005.

[70] S. Petronio, Brief Status Report on Communication Privacy Management Theory, Journal of Family Communication 13 (2013) 6–14. doi:10.1080/15267431.2013.743426.

[71] Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, United States of America, 2000.

[72] R. C. Mayer, J. H. Davis, F. D. Schoorman, An Integrative Model Of Organizational Trust, Academy of Management Review 20 (1995) 709–734. doi:10.5465/amr.1995.9508080335.

[73] D. H. McKnight, V. Choudhury, C. Kacmar, Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, Information Systems Research 13 (2002) 334–359. doi:10.1287/isre.13.3.334.81.

[74] D. Gefen, D. W. Straub, Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services, Omega 32 (2004) 407–424. doi:10.1016/j.omega.2004.01.006.

[75] T. Dinev, P. Hart, An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research 17 (2006) 61–80. doi:10.1287/isre.1060.0080.

[76] P. A. Pavlou, Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, International Journal of Electronic Commerce 7 (2003) 101–134. doi:10.1080/10864415.2003.11044275.

[77] S. San Martín, C. Camarero, How perceived risk affects online buying, Online Information Review 33 (2009) 629–654. doi:10.1108/14684520910985657.

[78] P. Lai, Design and Security impact on consumers' intention to use single platform E-payment, Interdisciplinary Information Sciences 22 (2016) 111–122. doi:10.4036/iis.2016.R.05.

[79] F. Bélanger, R. E. Crossler, Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, MIS Quarterly 35 (2011) 1017–1041. doi:10.2307/41409971.

[80] I. Pettersson, F. Lachner, A.-K. Frison, A. Riener, A. Butz, A Bermuda Triangle? A Review of Method Application and Triangulation in User Experience Evaluation, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA, 2018, pp. 1–16. doi:10.1145/3173574.3174035.

[81] W.-S. Tan, D. Liu, R. Bishu, Web evaluation: Heuristic evaluation vs. user testing, International Journal of Industrial Ergonomics 39 (2009) 621–627. doi:10.1016/j.ergon.2008.02.012.

[82] S. Hirsjärvi, P. Remes, P. Sajavaara, Tutki ja Kirjoita, 15 ed., Tammi, Helsinki, Finland, 1997.

[83] Finnish National Board on Research Integrity - TENK, Research Integrity (RI), 2024. URL: https://tenk.fi/en/research-integrity-ri.

[84] Finnish National Board on Research Integrity - TENK, Ethical review in human sciences, 2023. URL: https://tenk.fi/en/ethical-review/ethical-review-human-sciences.

[85] A. K. Singh, N. Upadhyaya, A. Seth, X. Hu, N. Sastry, M. Mondal, What Cookie Consent Notices Do Users Prefer: A Study In The Wild, in: Proceedings of the 2022 European Symposium on Usable Security, ACM, Karlsruhe, Germany, 2022, pp. 28–39. doi:10.1145/3549015.3555675.

[86] J. Tuomi, A. Sarajärvi, Laadullinen Tutkimus ja Sisällönanalyysi, revised ed., Tammi, Helsinki, Finland, 2018.

[87] V. Braun, V. Clarke, Thematic Analysis: a Practical Guide, Sage Publications, London, UK, 2022.