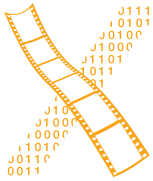

Chair for Computer Science 10 (Media Computing and Human-Computer Interaction)

RWTH AACHEN UNIVERSITY

Eliciting Countermeasures Against Deceptive Patterns

Bachelor's Thesis at the
Media Computing Group
Prof. Dr. Jan Borchers
Computer Science Department
RWTH Aachen University

by
Julia Kemp

Thesis advisor:
Prof. Dr. Jan Borchers

Second examiner:
Prof. Dr.-Ing. Ulrik Schroeder

Registration date: 13.06.2025
Submission date: 30.09.2025

Zentrales Prüfungsamt/Central Examination Office

RWTH AACHEN UNIVERSITY

Eidesstattliche Versicherung
Declaration of Academic Integrity

Kemp, Julia
Name, Vorname/Last Name, First Name

445313
Matrikelnummer (freiwillige Angabe)
Student ID Number (optional)

Ich versichere hiermit an Eides Statt, dass ich die vorliegende ~~Arbeit~~/Bachelorarbeit/ ~~Masterarbeit~~* mit dem Titel
I hereby declare under penalty of perjury that I have completed the present ~~paper~~/bachelor's thesis/~~master's thesis~~* entitled

Eliciting Countermeasures Against Deceptive Pattems

selbstständig und ohne unzulässige fremde Hilfe (insbes. akademisches Ghostwriting) erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt; dies umfasst insbesondere auch Software und Dienste zur Sprach-, Text- und Medienproduktion. Ich erkläre, dass für den Fall, dass die Arbeit in unterschiedlichen Formen eingereicht wird (z.B. elektronisch, gedruckt, geplottet, auf einem Datenträger) alle eingereichten Versionen vollständig übereinstimmen. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.
independently and without unauthorized assistance from third parties (in particular academic ghostwriting. I have not used any other sources or aids than those indicated; this includes in particular software and services for language, text, and media production. In the event that the work is submitted in different formats (e.g. electronically, printed, plotted, on a data carrier), I declare that all the submitted versions are fully identical. I have not previously submitted this work, either in the same or a similar form to an examination body.

Aachen, 29.09.2025
Ort, Datum/City, Date

Julia Kemp
Unterschrift/Signature

*Nichtzutreffendes bitte streichen/Please delete as appropriate

Belehrung:
Official Notification:

§ 156 StGB: Falsche Versicherung an Eides Statt
Wer vor einer zur Abnahme einer Versicherung an Eides Statt zuständigen Behörde eine solche Versicherung falsch abgibt oder unter Berufung auf eine solche Versicherung falsch aussagt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
§ 156 StGB (German Criminal Code): False Unsworn Declarations
Whosoever before a public authority competent to administer unsworn declarations (including Declarations of Academic Integrity) falsely submits such a declaration or falsely testifies while referring to such a declaration shall be liable to imprisonment for a term not exceeding three years or to a fine.
§ 161 StGB: Fahrlässiger Falscheid; fahrlässige falsche Versicherung an Eides Statt
(1) Wenn eine der in den §§ 154 bis 156 bezeichneten Handlungen aus Fahrlässigkeit begangen worden ist, so tritt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe ein.
(2) Straflosigkeit tritt ein, wenn der Täter die falsche Angabe rechtzeitig berichtigt. Die Vorschriften des § 158 Abs. 2 und 3 gelten entsprechend.
§ 161 StGB (German Criminal Code): False Unsworn Declarations Due to Negligence
(1) If an individual commits one of the offenses listed in §§ 154 to 156 due to negligence, they are liable to imprisonment for a term not exceeding one year or to a fine.
(2) The offender shall be exempt from liability if they correct their false testimony in time. The provisions of § 158 (2) and (3) shall apply accordingly.

Die vorstehende Belehrung habe ich zur Kenntnis genommen:
I have read and understood the above official notification:

Aachen, 29.09.2025
Ort, Datum/City, Date

Julia Kemp
Unterschrift/Signature

Contents

List of Figures and Tables

Abstract

The Internet plays an important role in almost every aspect of life for its increasing number of users. This opens up a lot of opportunities and motivations for manipulation, for example monetary gain. Deceptive patterns are one form of online manipulation: malicious interface elements that are designed to trick or deceive users into making decisions that are not in their best interest. To work against the threats of deceptive patterns, which include loss of money, time and privacy, there has been research on countermeasures. Still, current countermeasures are not comprehensive, not tailored to user preferences and not adaptive to future deceptive patterns.

In our work, we investigate the research question *How do users want countermeasures to handle deceptive patterns?* For this, we conducted a user study combining elicitation and focus group methodology, to first receive drawings of countermeasure design ideas and secondly investigate user preferences for countermeasures. Our in-person study had 18 participants and investigated 14 deceptive patterns.

We found that our participants' ideas mostly fell into the categories of visual, informational or automated countermeasures. Some of the ideas suggested in our study have already been researched and proven to be effective by existing literature, while other designs were completely new ideas. The focus group discussions revealed that participants value customizability, simplicity, transparency and autonomy in countermeasures. It is also important to have an uncomplicated setup process, a pleasant user experience and high trustworthiness. Additionally, we highlight different opinions about more controversial topics like hiding content or bright patterns. Our work lays the foundation for future research on specific countermeasures as well as user preferences, and is an opportunity to implement countermeasures that are in line with user ideas to help mitigate the negative effects of deceptive patterns.

Überblick

Das Internet spielt für eine steigende Nutzerzahl eine wichtige Rolle in fast jedem Lebensbereich. Dies bietet viel Angriffsfläche und Motivation für Manipulation, zum Beispiel finanzielle Gründe. Sogenannte *Deceptive Patterns* sind eine Form solcher Manipulation. Sie sind böswilliges manipulatives Design von Nutzerschnittstellen mit der Intention, Nutzer hereinzulegen oder zu täuschen, damit sie Entscheidungen treffen, die nicht in ihrem Interesse sind. *Deceptive Patterns* führen zu Verlust von Geld, Zeit und Privatsphäre für Nutzer, weswegen Gegenmaßnahmen erforscht werden. Aktuelle Gegenmaßnahmen sind nicht flächendeckend und nicht immer auf Nutzerpräferenzen angepasst.

Deswegen beschäftigen wir uns in dieser Arbeit mit der Forschungsfrage *Wie wollen Nutzer, dass Gegenmaßnahmen mit Deceptive Patterns umgehen?* Dazu führten wir eine Nutzerstudie durch, die Techniken von Elizitation und Fokusgruppeninterviews kombiniert, um Zeichnungen von Gegenmaßnahmen zu erhalten und Nutzerpräferenzen für Gegenmaßnahmen im Allgemeinen zu untersuchen. Unsere Studie hatte 18 Teilnehmer und untersuchte 14 verschiedene Deceptive Patterns.

Die Ideen unserer Teilnehmer lassen sich vor allem in die Kategorien "visuell", "informierend" oder "automatisiert" einordnen. Manche Ideen, die von unseren Teilnehmern vorgeschlagen wurden, wurden in bestehender Literatur bereits getestet und für effektiv befunden, während andere Bilder grundsätzlich neue Ideen waren. Die Diskussionen haben gezeigt, dass Nutzer bei Gegenmaßnahmen Wert auf Personalisierbarkeit, Einfachheit, Transparenz und Autonomie legen. Gleichzeitig wollen sie keinen komplizierten Einrichtungsprozess, kein nerviges Nutzererlebnis und keine Fehler der Gegenmaßnahme. Wir heben auch Meinungen zu kontroversen Themen wie das Verstecken von Inhalten oder umgedrehter Manipulation hervor. In unserer Arbeit legen wir die Grundlage für zukünftige Forschung zu spezifischen Gegenmaßnahmen und Nutzerpräferenzen, und geben Orientierungsmöglichkeiten, wie man Gegenmaßnahmen implementieren kann, um Nutzern gegen die Effekte von Deceptive Patterns zu helfen.

Acknowledgments

First of all, I would like to thank Prof. Dr. Jan Borchers and Prof. Dr.-Ing. Ulrik Schroeder for examining my thesis.

Thank you to René Schäfer for supervising my thesis. Your feedback was very valuable to me and you helped me learn a lot in the process. I appreciate the time you had for me.

A big thank you to everyone who participated in my user study. Your time and creativity made this thesis possible.

Finally, I want to thank my family, friends and boyfriend for their constant support, encouragement and feedback.

Conventions

Throughout this thesis we use the following conventions:

- The thesis is written in American English.
- The first person is written in plural form.
- Unidentified third persons are referred to in plural form.
- Study participants are referred to as Pxx, with xx being their assigned anonymous participant number.
- Deceptive pattern categories from our taxonomy are written in SMALL CAPS.
- Deceptive pattern names are written in *italics*.
- For better clarity, numbers are written as figures when referring to quantities (i.e. "8" instead of "eight").

DEFINITIONS:
Definitions of technical terms or short excursuses are set off in orange boxes.

Where appropriate, paragraphs are summarized by one or two sentences that are positioned at the margin of the page.

This is a summary of a paragraph.

Chapter 1

Introduction

With roughly 5.5 billion users[1] , the internet is an integral part of everyday life for a majority of the human population. Alongside its benefits, it also offers a platform for manipulation and deceptive practices. Companies wanting to sell products or user data can aim to influence users' important decisions concerning shopping behavior or privacy settings through manipulative design [Mathur et al., 2019; Nouwens et al., 2020].

The internet brings many opportunities to manipulate its users

1.1 Deceptive Patterns

DECEPTIVE PATTERN:
Mathur et al. [2019] define deceptive patterns as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions."

Definition: *Deceptive Pattern*

[1] `https://www.statista.com/topics/1145/internet-usage-worldwide/`, *last accessed August 23, 2025*

The field of research is still young and growing

The area of deceptive patterns has evolved to include many definitions and taxonomies since Brignull [2023] first brought up the issue in 2010.
As a still expanding field, new aspects are regularly being introduced and researched, for example the effects of combining multiple deceptive patterns [Gray et al., 2025].

Deceptive patterns are effective at getting users to perform actions that are not in their best interest

Research has found that deceptive patterns are very effective at influencing users: When presented with a manipulative cookie consent notice, less than half of users have success with selecting their preferred consent option [Habib et al., 2022]. Combinations of patterns are able to double the percentage of users that perform an unwanted action, and less educated users are more vulnerable [Luguri and Strahilevitz, 2021].

User awareness is neither widespread enough or guaranteed protection

According to Di Geronimo et al. [2020] the majority of users are not aware of or able to detect deceptive patterns, possibly because they are so common that users are simply used to their presence. Additionally, research by Bongard-Blanchy et al. [2021] shows that deceptive pattern awareness does not predict the ability to resist them.

Since deceptive patterns lead users to lose money, privacy and time [Lewis and Vassileva, 2024], while users are also unaware of their effects, there is a need to find ways to counteract them.

1.2 Countermeasures

Countermeasures can mainly be educational, shaming, laws or technical

The four main ways of protecting users from deceptive patterns are raising awareness, publicly shaming or boycotting companies, laws, and technical countermeasures [Brignull, 2023; Maier and Harr, 2020; Schäfer et al., 2023]. As Brignull [2023] explains, laws are a fundamental component of countering the threat deceptive patterns pose to users, but currently not comprehensive or enforced enough. With awareness not being sufficient for users to consistently resist deceptive patterns and companies profiting from them, this leaves a gap in user protection that technical countermeasures aim to fill.

There are different ways to implement technical countermeasures, most of which require automated detection of deceptive patterns. Research by Curley et al. [2021] and Mathur et al. [2019] shows that this is possible. After detecting the deceptive patterns, software tools like browser extensions can deal with them in different ways. These include adjusting user flow [Lu et al., 2024], automatically enforcing user preferences [Khandelwal et al., 2021] or visually changing the web page [Schäfer et al., 2023].

Technical countermeasures detect and handle deceptive patterns in the form of software

The opposite of deceptive patterns are user-centered patterns, which aim to not manipulate the user at all [Brignull, 2023; King and Stephan, 2021; Potel-Saville and Da Rocha, 2023]. Another option is using the same manipulative tactics as deceptive patterns to nudge the user towards the more user-friendly option, which is called bright patterns [Graßl et al., 2021].

The non-manipulative counterpart to deceptive patterns are fair patterns, while bright patterns manipulate the user with good intent

Research by Schäfer et al. [2023] shows that user opinions about countermeasure strategies such as hiding or highlighting the manipulation vary strongly. When exploring user ideas for countermeasures, Lu et al. [2024] found that they can be sorted into the categories interface design change, user flow adjustment and behavioral outcome reflection. While there is some general exploration of user ideas [Lu et al., 2024], it has not been done in depth and covering all deceptive patterns. Since user ideas can be good reference points for how to design interfaces [Good et al., 1984], investigating them could be valuable input for future countermeasure design. Generating ideas and researching user preferences for countermeasures is the goal of this thesis.

User preferences for countermeasures vary

New deceptive patterns are constantly being introduced and researched, such as social media specific patterns [Mildner et al., 2023]. There are also new characteristics that researchers need to consider when designing countermeasures, such as temporality [Gray et al., 2025] and contextual vulnerability [Alsebayel et al., 2024]. For these new deceptive patterns and aspects, there are no specific countermeasures yet, which is one of the gaps in research this thesis aims to fill.

New deceptive patterns and characteristics need new countermeasures

1.3 Outline

This thesis focuses on user ideas and preferences for countermeasures

This thesis aims at generating ideas for countermeasures against deceptive patterns and understanding user preferences for countermeasure approaches and characteristics. We create a taxonomy of deceptive patterns oriented towards countermeasures and conduct a user study using elicitation techniques and focus group interviews.

In Chapter 2 "Related Work", we go over previous research on deceptive patterns and countermeasures, as well as existing taxonomies of deceptive patterns. Based on this, we construct a new taxonomy and cover our user study structure in Chapter 3 "User Study". After discussing the study procedure and data collection goals, we present the results of the study, including specific countermeasure designs as well as discussion points. Chapter 4 "Discussion" builds on this by evaluating our findings, comparing them to previous work and highlighting their implications for deceptive pattern research, as well as our study's limitations. Finally, in Chapter 5 "Summary and Future Work", we summarize our contributions and examine how future work can build on our results.

Chapter 2

Related Work

In the following sections, we provide an overview of previous research on deceptive patterns and why they pose a problem to individual users and society. Then, we discuss countermeasures that have already been implemented and tested, and argue why there is a need for further research on countermeasures.

2.1 Deceptive Patterns

Deceptive patterns have been researched since 2010

Deceptive patterns were first introduced by Brignull [2023] as "dark patterns" in 2010. Like Brignull [2023], we will use the term "deceptive pattern" in this thesis to avoid racist associations, and only use "dark patterns" in direct quotes. Originally, he defined them as "a user interface that has been carefully crafted to trick users into doing things, such as buying insurance with their purchase or signing up for recurring bills". In the same year, Conti and Sobiesk [2010] discussed the topic of violating good design principles to manipulate or exploit the user, characterizing these interfaces as malicious. Even though they did not use the term "deceptive pattern", they described examples of manipulative interfaces, and argue that the key point in recognizing malicious design is the designer's intent to worsen the user experience to prioritize their own goals.

Deceptive patterns are intentional manipulation of users

Similarly, Gray et al. [2018] place a lot of importance on designers' responsibilities and the need for them to consider ethical issues. They define deceptive patterns as instances where designers implement deceptive elements to work around the user's best interest using their knowledge of human psychology. However, they consider unintentionally poor design as something different, naming the phenomenon "anti-pattern" and draw a clear distinction based on the intentions behind the design.

There are different deceptive patterns in different contexts

There are different deceptive patterns depending on context, for example a shopping website might have the goal of getting the users to spend more money and manipulate them accordingly, while a social networking site profits from users spending more time on the site or sharing their data [Mildner and Savino, 2021].

2.1.1 Taxonomies

There are many different taxonomies trying to provide common ground for research

Since the early definition of deceptive patterns, many researchers have created taxonomies to classify the different types of manipulative design. In their early work on malicious interfaces, Conti and Sobiesk [2010] introduce eleven categories of designs: *Coercion, Confusion, Distraction, Exploiting Errors, Forced Work, Interruption, Manipulating Navigation, Obfuscation, Restricting Functionality, Shock* and *Trick*. Many of these categories reappear in later taxonomies that are explicitly about deceptive patterns.

Deceptive patterns can be categorized by their manipulative tactics or characteristics

Another influential taxonomy by Mathur et al. [2019] classified deceptive patterns by their characteristics: *asymmetric, covert, deceptive, hides information* and *restrictive*. They also refer to the cognitive biases deceptive patterns abuse, naming different psychological effects that allow deceptive patterns to work. Using these, they came up with the categories *Sneaking, Urgency, Misdirection, Social Proof, Scarcity, Obstruction* and *Forced Action*.

Another way to talk about deceptive patterns was introduced by Bongard-Blanchy et al. [2021], which differentiates between three strategies: *coercive, nudging* and *deceptive* patterns. They also considered that each strategy had a different cost to resisting the pattern.

There are different perspectives to consider when talking about deceptive patterns

Mathur et al. [2021] describe different perspectives on deceptive patterns. Firstly, they name the *individual welfare* perspective, which considers problems that deceptive patterns cause for individuals, such as financial loss, invasion of privacy and cognitive burden. *Collective welfare* revolves around the effects of deceptive patterns on society. Furthermore, they also regard *regulatory objectives* and *individual autonomy* as perspectives. For *individual autonomy*, they add the concern that from this perspective, every interface that interferes with decision-making in any way is classified as a deceptive pattern, and that there needs to be a line between persuasion and violating autonomy.

The ontology by Gray et al. [2024] converges other important taxonomies and sorts deceptive patterns into high-, meso- and low-level categories

A recent ontology by Gray et al. [2024] focuses on converging other important taxonomies to create a shared language for deceptive pattern research. They sort deceptive patterns into the high-level categories *Obstruction, Sneaking, Interface Interference, Forced Action* and *Social Engineering*, which are general strategies of manipulation. Each of these categories is then split into meso-level patterns, which describe the approach and are further separated into low-level patterns which are specific means of execution. According to Gray et al. [2024], low-level patterns can mostly be detected through technical means.

Social networking sites have specific deceptive patterns

Apart from general taxonomies of deceptive patterns, there are also ones for specific situations or purposes. For example, Mildner et al. [2023] proposed a taxonomy of deceptive patterns that appear specifically on social networking sites. They identified the categories *interactive hooks, social brokering, decision uncertainty, labyrinthine navigation* and *redirective conditions*. They then organized them into two overarching strategies on a higher level: *engaging* and *governing*, which can be applied more broadly.

Deceptive patterns can be paired up with corresponding non-manipulative patterns

Potel-Saville and Da Rocha [2023] focused on a taxonomy of deceptive patterns with corresponding fair patterns. They proposed the pairs *harmful default - protective default, missing information - adequate information, maze - seamless path, push & pressure - non-intrusive information, misleading or obstructing language - plain and empowering language, more than intended - free action* and *distorted UX - fair UX*.

Designers' perspectives can help understand the manipulation

Bösch et al. [2016] explored the techniques used in deceptive patterns by taking the perspective of the perpetrators to better understand the underlying mechanisms. They col-

Current taxonomies are not well-suited for user education or countermeasure creation

lected eight privacy deceptive pattern strategies opposing to privacy preserving principles: *Maximize, Publish, Centralize, Preserve, Obscure, Deny, Violate* and *Fake*. Ye et al. [2025] built an experiential learning platform. In the process of testing it with users, they came to the conclusion that the ontology by Gray et al. [2024] was not suited for this purpose. Participants had trouble memorizing the categories and classifying the patterns, leading Ye et al. [2025] to the conclusion that there is a need for a user-friendly taxonomy. To our knowledge, another angle a taxonomy could tackle that has not been proposed yet is a taxonomy built around countermeasures and how specific deceptive strategies might be similar to counter.

2.1.2 Effects on Users

To understand the danger deceptive patterns pose, one has to look into how they affect user interactions and influence users.

Why deceptive patterns work can be explained by various psychological models

To comprehend how deceptive patterns influence users, one has to know why humans behave the way they do. Here, we will focus on the Fogg Behavior Model [Fogg, 2009], which explains behavior as a product of three factors: motivation, ability and triggers. Especially with computers, triggers can cause users to act impulsively. In addition to using social cues, this can be used for persuasion and to change behavior [Fogg, 2002, 2009]. Another way one can consider the effect of manipulation is by distinguishing between influencing choice and behavior. Hansen and Jespersen [2013] explain that choice is influenced when a nudge manipulates the user's controlled, system 2 thinking, while behavior is influenced through manipulation of automatic, system 1 thinking. Both are represented in deceptive patterns.

Deceptive patterns effectively prevent users from achieving their goals in interactions

There has been a lot of research showing that deceptive patterns work. For example, when investigating privacy consent notices, Habib et al. [2022] found that less than half of the participants selected their preferred option. Nouwens

et al. [2020] examined the influence of a cookie banner's design on the acceptance rates and discovered that Obstruction increased consent by more than 20%, while providing more options decreased consent by up to 20%. Furthermore, the default option is very powerful in influencing users' decisions [Singh et al., 2022] and combinations of deceptive patterns can double the percentage of users that accept or buy something they did not want [Luguri and Strahilevitz, 2021].

Convenience outweighs privacy concerns and manipulation leads to automatic responses

The Privacy Paradox is a phenomenon where users claim to value their own privacy, but do not act accordingly. Graßl et al. [2021] and Jung et al. [2022] found that many users do not read privacy policies or consent notices and just accept them automatically. Jung et al. [2022] argue that this results from the placement, format and design of the information, which is meant to nudge users towards uninformed acceptance. Similarly, Inal et al. [2024] observed that participants in their study did not read the text on the interface. They investigated the influence of deceptive pattern usage on the ease of use of an interface through tracking gaze fixations. The design variants containing some or many deceptive elements were more challenging than the fair design variant, with the very manipulative design variant having the highest total interaction duration and number of fixations.

Some user groups are more vulnerable than others

Different user groups are influenced by deceptive patterns differently. Luguri and Strahilevitz [2021] found that less educated users are more vulnerable to deceptive patterns. While children have been shown to have some understanding of manipulation [Schäfer et al., 2025], they lack understanding of how the deceptive patterns work and are sometimes limited to recognizing the ones they already know about [Renaud et al., 2024]. Together with the increased time they spend on the internet, this makes them a vulnerable group to the effects of deceptive patterns [Renaud et al., 2024]. Other findings show that older people may be more susceptible to deceptive patterns as well [Directorate-General for Justice and Consumers (European Commission) et al., 2022; Bongard-Blanchy et al., 2021]. Mildner et al. [2025] considered how ADHD might influence recognition and avoidance of deceptive patterns and, through a user study, came to the conclusion that there was no significant difference between recognition of deceptive patterns by ADHD and non-ADHD individuals. However, they also

noted that ADHD individuals were able to avoid specific patterns more often, and that the ADHD group entered more data in total, suggesting to them a stronger vulnerability to disclose more personal data than required.

Variables such as subtlety, trustworthiness, frequency of occurrence and user frustration can influence how effective a deceptive pattern is

Other factors for the impacts of deceptive patterns include that more subtle manipulations have been proven to be more effective [Keleher et al., 2022], possibly because they do not receive negative backlash from users and thus appear to sway more users without consequences [Luguri and Strahilevitz, 2021]. Bhoot and Shinde [2020] found "variables of identification" which can influence how strongly a pattern works. They list frequency of occurrence, trustworthiness of the site, misleading behavior, level of frustration and physical appearance of user interfaces.

2.1.3 User Perspectives

Another aspect that has seen extensive research are users' perceptions of deceptive patterns and their opinions.

Users are generally not aware of deceptive patterns

One important part of considering user perspectives is user awareness. Research by Bongard-Blanchy et al. [2021]; Di Geronimo et al. [2020] and Seaborn et al. [2024] has shown that the majority of users is not aware of deceptive patterns, and two thirds of deceptive patterns are unnoticed in interactions. One reason might be that deceptive patterns are very common and users are simply used to them [Di Geronimo et al., 2020]. Other researchers have found that awareness has started to spread, but is not comprehensive yet [Bhoot and Shinde, 2020; Maier and Harr, 2020].

According to Keleher et al. [2022], experts often overestimate users' ability to recognize manipulation, as users do not understand the underlying mechanisms.

Users cannot resist deceptive patterns consistently, even when they know about them

Even if users recognize deceptive design, Bongard-Blanchy et al. [2021] observed that they are not consistently able to resist the manipulation. Hinds et al. [2020] also discovered that individual users often consider themselves to be exempt from the manipulation, as they consider themselves immune to targeted advertisements and similar things.

Deceptive patterns evoke negative emotions in users

From a user perspective, deceptive patterns are not always deceptive but rather disruptive [Seaborn et al., 2024]. While users may not always recognize deceptive patterns, they notice when their interactions do not have the intended outcome and react accordingly. According to research by Luguri and Strahilevitz [2021], aggressive manipulation is more likely to receive a strong negative reaction from users than subtle patterns, but only when the users try to resist the manipulation.
Gray et al. [2020] found that users engage in ethical discourse about manipulative design and generally feel annoyed when they notice it, blaming the website designers.
User satisfaction with their interactions does not only take the form of annoyance. Bhoot and Shinde [2020] and Seaborn et al. [2024] discovered that generally, users assume good intentions when running into deceptive patterns on the internet and tend to blame their own incompetence before the website designer. This trust in the website is increased by appealing user interface (UI) design and in turn leads users to willingly accept deceptive patterns when they already trust a company [Bhoot and Shinde, 2020]. On the other hand, Maier and Harr [2020] found that their participants blame the businesses that use them for the consequences rather than themselves. According to Seaborn et al. [2024], some patterns were more acceptable to participants than others, depending on trust in social indicators or the level of irritation the pattern provoked.
However, Bhoot and Shinde [2020] also observed that users get frustrated when encountering deceptive patterns and trust the website less afterward. Both Jung et al. [2022] and Alsebayel et al. [2024] found that users voice privacy concerns when encountered with questionable design practices and monetization tactics, especially in health apps where users are in a very vulnerable context. Another point that participants raised concerns about was not understanding and more importantly not trusting privacy consent purpose namings [Kyi et al., 2024]. Generally, Maier and Harr [2020] discovered that users perceive deceptive patterns as sneaky and dishonest, but carry a resigned attitude, especially when considering their dependency on the services that use them.

Users often do not change their behavior, even when they know about the manipulation and feel annoyed

The last interesting aspect of user perspectives we want to consider is their behavior. When they recognize manipulative design, Gray et al. [2020] found that users feel annoyed and discontinue the use of the application.
In contrast, multiple studies had the result that user convenience outweighs previously raised privacy concerns [Jung et al., 2022; Porcelli et al., 2024] and that users often accept all cookies out of habit or to choose the easiest option [Habib et al., 2022]. When investigating the aftermath of the Cambridge Analytica scandal, Hinds et al. [2020] discovered that users did not express concerns about the incident and did not change their behavior by deleting their accounts or changing their privacy settings to prevent similar manipulation.
Conti and Sobiesk [2010] posed that users will analyze the costs and benefits of their interaction with a malicious interface,and decide accordingly whether they will continue using the application.

2.1.4 Evolution

The field is still evolving

As a relatively young field of research, it is still evolving as designers are coming up with new ways to manipulate users, researchers are discovering and discussing new aspects of manipulation and countermeasures are being developed.
This change can already be seen when considering the early definition of deceptive patterns by Brignull [2023] as "a user interface that has been carefully crafted to trick users into doing things, such as buying insurance with their purchase or signing up for recurring bills". While the aspect of tricking users remains, the applications have broadened greatly since the phenomenon was first discussed, now including countless ways to cost users money, privacy and time [Lewis and Vassileva, 2024].

New aspects are being researched, such as new deceptive patterns and context-specific characteristics

A new aspect to consider that was brought up by Gunawan et al. [2021] is comparing websites and mobile apps. One modality may contain more deceptive patterns than the other, or specific types might be more common. They urge to consider the impact of platform affordances, capabilities

and design norms to accurately gauge how manipulative a service is. They found that modality does affect deceptive pattern prevalence, type and other characteristics.
An example of discovering a new form of a deceptive pattern was published by Mildner and Savino [2021], investigating Facebook's "privacy checkup". Facebook offers a guided settings feature, curating which settings a user will manage. This could be used to intentionally keep users from certain settings and therefore considered as a novel deceptive pattern [Mildner and Savino, 2021]. More generally, Mildner et al. [2023] have done research on deceptive patterns specific to social networking sites, such as interface designs that encourage uncontrolled use of social media or complicate data protection. These are currently unregulated. In their work, Mildner et al. [2023] found instances of deceptive design that were not identified in earlier research, showing the constant evolution of the field.
While many researchers consider users' vulnerability as a set state, Alsebayel et al. [2024] urge to consider contextual vulnerability as an important aspect. They explain that users' vulnerability to manipulation is a dynamic construct and can change according to their circumstances, which they argue highlights the need to capture deceptive patterns in context.

Recently, the aspect of temporality was introduced

Very recently, Gray et al. [2025] introduced another interesting aspect of deceptive patterns that had not been considered before. They highlighted the effects of temporality by describing three levels of how deceptive patterns can interact in a system: intra-page, inter-page and system level. They explain that having multiple deceptive patterns in an interaction increases the complexity and that they amplify each other to function even stronger.

2.2 Countermeasures

Countermeasures can be educational, regulatory, technical or boycotting companies

Taking into account how much of a problem deceptive patterns pose to users through their effectiveness and malicious usages, research on countermeasures is very important. To weaken the effects of deceptive patterns, measures such as curtailing digital surveillance, problematiz-

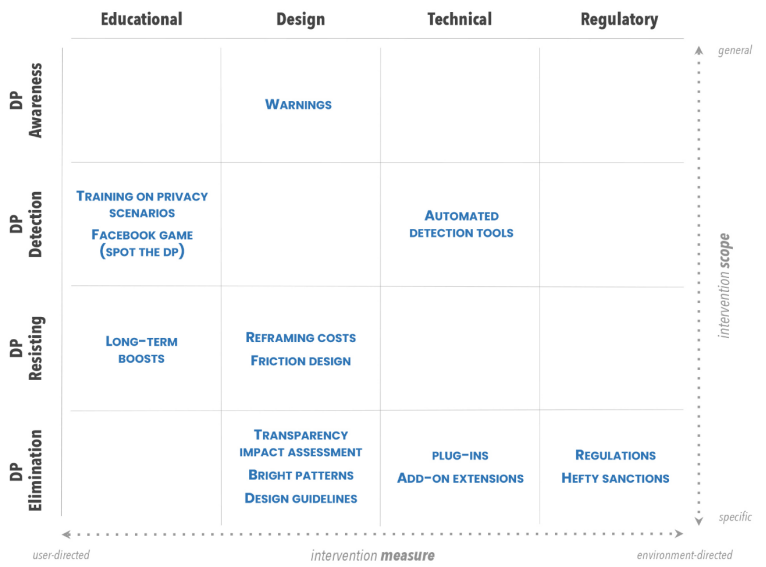

Figure 2.1: Deceptive Pattern Intervention Space by Bongard-Blanchy et al. [2021]. All countermeasures fall into this matrix.

ing personalization and promoting awareness have been suggested [Susser et al., 2019]. Generally, researchers have identified four main ways of dealing with deceptive patterns directly: educating users, putting pressure on companies, laws and technical countermeasures [Brignull, 2023; Schäfer et al., 2023]. This raises the question of responsibility: what are users responsible for, and what are organizations and platforms responsible for? Hinds et al. [2020] argue that users should not be fully responsible as it would create even more pressure, while placing the responsibility fully on organizations could lead to a decrease in trust by users and a feeling of lacking control.
Bongard-Blanchy et al. [2021] describe four different possible approaches for interventions: raising awareness, facilitating detection, bolstering resistance and eliminating them from online services. They further differentiate the approaches by acting on the user or the environment and, based on that, identify the actors that should implement countermeasures, picking up the subject of responsibility. Their intervention space results in the matrix shown in Figure 2.1.

Legal regulations could be an effective countermeasure but face many challenges

The perhaps simplest solution to the problem deceptive patterns pose would be outlawing them, which would in theory prevent them from doing any more harm. There have been some attempts at legal regulations by various countries and organizations, as outlined by Brignull [2023]. However, there are problems with this approach. As Kelly and Burkell [2024] highlight, regulatory frameworks need to rely on detecting patterns. By design, deceptive patterns and the point at which user autonomy is openly affected are hard to detect and quantify [Kelly and Burkell, 2024]. Even if some patterns are clearly prohibited by legal regulations, others are permitted, not addressed or hard to classify due to lack of guidance in the legislation [Tran et al., 2025], and combinations of deceptive patterns may make even subtle or seemingly harmless ones become a problem [Kelly and Burkell, 2024]. Tran et al. [2025] researched whether websites that were subject to the California Consumer Privacy Act (CCPA) employed deceptive patterns, and found at least one on about 200 of 292 websites that they looked at. Some of the patterns they found were explicitly prohibited by the CCPA, others took advantage of legal loopholes, showing how ineffective current legal regulations are at stopping deceptive patterns. While the General Data Protection Regulation (GDPR) made cookie consent notices mandatory to protect users' privacy, many companies utilize deceptive patterns in them [Nouwens et al., 2020].
Similarly, companies often do not suffer consequences even when the public is aware of their deceptive practices [Bongard-Blanchy et al., 2021]. This takes away boycotting as an effective option, too.

User education can take different forms and can help improve understanding

Educating the user or providing them with information can be implemented in different ways. One option is to provide information about the deceptive pattern right where the user encounters it to warn and inform them [Schäfer et al., 2023], which allows them to gain transferrable knowledge [Luguri and Strahilevitz, 2021]. Ye et al. [2025] built an experiential learning platform to teach users about deceptive patterns and their consequences. They simulated real-world deceptive pattern cases and coping strategies, and found that participants were significantly better at coping with deceptive patterns after using the platform. Their main positive qualitative results were improved un-

derstanding and experience in dealing with deceptive patterns. While users found classifying and memorizing deceptive patterns challenging, they arrived at the conclusion that experiential learning-based deceptive pattern education is effective. However, they also highlight that a user-friendly taxonomy and more practical solutions for deceptive patterns are needed.
Other, more general options include educating users through credible and independent educational channels such as NGOs, governments or educational institutions [Jarovsky, 2018]. Another way of teaching users to recognize and avoid deceptive patterns are serious games. While they are not widely used yet, researchers like Fiedler et al. [2025] and Kronhardt and Gerken [2024] have argued and shown that they have the potential to improve users' detection skills.

There is a psychological basis to countermeasures

Other than that, there are more technical options for countermeasures, which can be based on psychological concepts. Ozkaramanli et al. [2017] explains that solving self-control dilemmas can be reached by demotivating immediate desires or motivating long-term goals, which can be done through adding new sources of displeasure or pleasure, making potential losses or gains tangible and creating barriers or enablers. These principles can also be applied to behavior change concerning deceptive patterns.
When designing countermeasures, Jarovsky [2018] emphasize the importance of not making them paternalistic. Instead, they should help the user make better decisions, for example through education, consumer-friendly language, formatting requirements, standardized privacy notices and more data collection options.

Bright patterns manipulate the user in their own interest

As a way of reversing the effect of deceptive patterns, researchers have looked into so-called bright patterns and nudging, which use the same manipulative techniques that deceptive patterns rely on, but try to manipulate the user for their own good rather than prioritizing the designer's interests [Bongard-Blanchy et al., 2021]. Bermejo Fernandez et al. [2021] define nudging techniques as tactics that designers can use to help users make more informed decisions. In a study on cookie consent notices, they observed that nudging can increase the probability that a user

changes the default setting by 14%. While Graßl et al. [2021] similarly found that bright patterns managed to influence users effectively, their participants also reported low perceived control.
There is an argument that bright patterns are unethical and violate the user's autonomy [Strauss, 2000]. Lu et al. [2024] argue that users should be offered multiple intervention options as well as information on deceptive patterns to make autonomous decisions. In a probe study, they found that providing knowledge about specific instances of deceptive patterns allowed users to gain transferrable knowledge and that the ability to modify existing interfaces improves the user's perception of their own autonomy. They also indicate that goals and usage context determine users' preferred UI enhancements.

Fair patterns do not manipulate the user at all

Described by Brignull [2023] as the counterpart to deceptive patterns are fair, light or user-centered patterns. They are non-coercive design that respect the user and the law [Brignull, 2023; King and Stephan, 2021]. Potel-Saville and Da Rocha [2023] created a taxonomy of deceptive patterns with corresponding fair patterns for better design practices. For example, they replace "harmful defaults" with "protective defaults" and "missing information" with "adequate information". While advocating for fair design, King and Stephan [2021] warn that simply giving more checkboxes or buttons does not solve the problem and list criteria for non-coercive design: existing consent options, consent options placed at equal prominence and with equal design, and not having a default option.

Countermeasures are evolving in reaction to deceptive patterns

Lastly, there are many new areas where countermeasures can be explored. Preuschoff et al. [2025] recently brought up the effects of group behavior on dealing with deceptive pattern and proposed considering this for countermeasures, for example through simulating an additional team member. With countermeasures being a reactive field by design, there is of course always possibility for research concerning new deceptive patterns and aspects of manipulative design, such as temporality [Gray et al., 2025] or context specific characteristics. Due to this, there is always a demand for new countermeasures and a need to keep investigating user preferences.

2.2.1 Detection

Technical countermeasures require automated detection

When aiming for automated removal or handling of deceptive patterns, an obvious requirement is automated detection and recognition of the patterns as a first step. There are different things that need to be considered for this, for example whether it is even possible for every deceptive pattern. Curley et al. [2021] tried to answer this question by investigating which patterns can be detected in an automated way, manually, or not at all. They came to the conclusion that it depends on the pattern, making automated detection difficult. As a way of assessing the malice of an interface using screenshots, Mildner et al. [2023] tested applying questions based on the characteristics of deceptive patterns from the taxonomy by Mathur et al. [2019]. Asking these questions, they evaluated the interface using a Likert scale and calculated the resulting values into a single digit, which was the final maliciousness rating.

Automated detection can be achieved through web crawlers, Artificial Intelligence or analyzing a website's code

For automated detection, there are multiple technical ways. Mathur et al. [2019] tested a web crawler, and both Hasan Mansur et al. [2023] and Chen et al. [2023] used computer vision and natural language processing to handle visual and textual content. Their respective positive results demonstrate that developing automated deceptive pattern detection tools is feasible.
When trying to utilize Artificial Intelligence (AI) to detect deceptive patterns, Mills and Whittle [2023] highlighted three main approaches. Firstly, they suggested "AI Vision", where the Large Language Model (LLM) would be provided with images and judge them using different personas, which they found to be promising. The second one was called "Choose your own adventure" and consisted of providing the LLM with detailed text input to let it choose what to do, which made the technical side very simple and was shown to have potential. Lastly, they suggested trying to incorporate AI functionality into a web crawling program, which failed due to technical challenges. Soe et al. [2022] also specified challenges when trying to use machine learning to automatically recognize deceptive patterns, namely the representation of the patterns, detection of different aspects of the patterns and the fact that some

types of patterns are easier to recognize than others.
As another way to implement detection without using AI, Hausner and Gertz [2021] proposed an extension that considers the DOM tree of the website and treats each node as a potential deceptive pattern. The extension can then detect whether two similar buttons are presented differently using CSS. While this could for example detect *Visual Prominence*, it would not work for *Roach Motel* or similar patterns [Hausner and Gertz, 2021].

Some manipulative tactics are used for good, but they are hard to differentiate from bad usages

Schlolaut et al. [2024] considered the interesting aspect of distinguishing between malicious manipulation and positive nudges towards better decision. They come to the conclusion that from a technical perspective, there is no difference between the two, as they are implemented using the same techniques, which makes it impossible to distinguish between them using a web crawler. This is important when considering whether all manipulation is bad or whether some positive nudges play an important role in interactions. For example, Lewis and Vassileva [2024] argue that Obstruction can play a vital role in protecting users from mistakes and that some form of visual ranking of options is necessary to allow a comprehensive overview over a page.

To summarize, while automated detection of deceptive patterns is an area that still faces challenges, it has shown promising results and can be assumed to work when designing technical countermeasures.

2.2.2 Technical Countermeasures

Visual countermeasures to deceptive patterns include highlighting, hiding or lowlighting deceptive patterns

One way of disarming deceptive patterns is visually. Schäfer et al. [2023] investigated user preferences for a range of visual countermeasures consisting of highlighting, highlighting and explaining, lowlighting (making it less prominent), hiding as well as hiding and marking a deceptive pattern. They found that user preferences vary strongly, leading to the conclusion that customizability is important for countermeasures.

Highlighting and explaining deceptive patterns shows promising results

Especially the idea of highlighting the deceptive pattern has received a lot of research. Adorna et al. [2024] and Raju et al. [2022] created similar extensions that showed alerts or marked deceptive patterns in cookie banners, with a high accuracy and positive user acceptance tests [Adorna et al., 2024]. In their user study, Schäfer et al. [2023] observed that users want explanations and prefer highlighting with an explanation over just highlighting a deceptive pattern. Their participants also said that it could make a website seem less trustworthy and increase visual clutter. In another study, Schäfer et al. [2024] found that participants preferred highlighting and explaining over other countermeasures for situations where there could be hidden costs or for patterns like Sneaking and Forced Action.

User preferences on hiding deceptive patterns are mixed

There is also the option of hiding the deceptive pattern completely, or making it less visually prominent, for example by graying it out. Schäfer et al. [2023, 2024] found that hiding was the most controversial countermeasure they tested with participants. On the one hand, it produces no additional visual clutter and turns the deceptive pattern into a fair pattern. On the other hand, participants did not want countermeasures to silently hide information and also raised concerns that it would make the website seem more trustworthy. They preferred it over other countermeasures in situations where the manipulation made one option seem superior, for example the deceptive pattern Interface Interference. Making the pattern less visually prominent ("lowlighting") overall received good rankings and was not strongly preferred over other countermeasures [Schäfer et al., 2023].

Redesigning interfaces can have a strong effect on user behavior

In a study on cookie consent notices, Bermejo Fernandez et al. [2021] tested different ways to redesign the notice. The countermeasures they showed participants were having options for four cookie categories and having a color-based bar to visualize the number of enabled cookies. They found that the colored bar had a stronger effect on their participants' behavior.

The efficiency of countermeasures can depend on context

Apart from highlighting, hiding and redesigning, visually adding content like alerts or friction is another way to counter deceptive patterns. Meinhardt et al. [2025] tested

the effect of a user's emotional state and social situation on the effectiveness of friction countermeasures for the pattern Infinite Scrolling. They found that interventions were more effective when users were surrounded by strangers, that users felt less resistance when they were tired, and that more severe or multi-step interventions might be necessary when at home or in bed.

There has been research on automatically adjusting settings according to user preferences

Another area where technical countermeasures can act are privacy settings, which often suffer from usability and reachability issues. To provide users with control over their data, Khandelwal et al. [2021] present "PriSEC", which uses machine learning techniques to automatically enforce web privacy controls. It finds privacy controls, presents them in a searchable, centralized interface and applies them with very little user action needed. It is precise in over 90% of control pages and, in a user study, showed an average reduction of 3.75 times of the time it took users to adjust privacy settings compared to the unaltered website.

Cookie consent notices can be denied automatically to reduce user effort

Khandelwal et al. [2023] also designed a system for automatically dealing with cookie consent notices and denying all non-essential cookies. "CookieEnforcer" can generate the required clicks to deny all cookies in 93.7% of the tested cases, and is stable and scalable according to its behavior on the top 100,000 websites Khandelwal et al. [2023] tested it on. Furthermore, in a user study, it significantly reduced user effort when interacting with cookie banners.
Similarly, Porcelli et al. [2024] present the user support tool "UPPMS" to handle consent notices and deceptive patterns for the user. They created a process for users with any knowledge level to create a standardized personal privacy policy. The extension then automatically applies this to every website the user visits by interacting with cookie banners. They use customized LLMs and aim to reduce information overload and decision fatigue for the user. For future work, they suggest that the extension could also suggest products and services matching the user's privacy needs, and that it could also be extended to other contexts where users may encounter deceptive patterns or difficulties in expressing their preferences.

2.2.3 User Ideas

There has been some research on user ideas and preferences

There has been research on ideas suggested by users, either by users bringing them up during studies or by researchers explicitly asking for them.
In a study by Maier and Harr [2020], participants brought up countermeasure ideas. Mainly, they said that deceptive patterns may not be stopped, so users need to focus on "how to best live with them". Other suggestions include being careful, warning users of existing deceptive patterns, software like ad blockers, laws, public shaming, using alternatives and leaving the internet completely.
Singh et al. [2022] investigated what factors were important for an interface. Users value ease of use, conciseness, the ability to customize, high speed, clarity and transparency.

Early user suggestions include blocking the patterns' functionality or browsing anonymously

Even when first bringing up the issue, Conti and Sobiesk [2010] asked users what measures they took or suggested to deal with malicious interfaces. The answers were focused around blocking the deceptive patterns' functionality or browsing anonymously.
In a workshop where users were asked to come up with countermeasure ideas, Lu et al. [2024] found three main strategies for deceptive pattern intervention. First was interface design change, where participants modified interface components and layouts to eliminate malicious design. Second was user flow adjustment, which prevents users from falling into behavioral traps. The third strategy was behavioral outcome reflection. For example, users wanted to know how many times they had been affected by deceptive patterns on a certain website and adjust their usage of the service accordingly.

There is a need for more research on countermeasures

As we have seen in Section 2.1.4 "Evolution", deceptive patterns are constantly evolving. Due to this, there is always need for new countermeasures. To our knowledge, there are no approaches that take a step towards countering future deceptive patterns, which is one topic where our thesis aims to close the gap in research. Additionally, there has not been a lot of investigation into user ideas for countermeasures, which should be rectified, as we argue in 3.2 "Method".

Chapter 3

User Study

In this chapter, we describe our study design, followed by a presentation of the results.

3.1 Research Question

With this thesis, we aim to answer the following research question.

RQ How do users want countermeasures to handle deceptive patterns?

There are two main aspects to consider for this: user ideas and user preferences.

3.2 Method

We combine elicitation and focus group methodology for our study

To answer our research question, we wanted to conduct a user study in two parts: first, a elicitation-style part where participants would be asked to draw countermeasures for a certain deceptive pattern to generate ideas and then discuss them to determine the favored ones. Secondly, we wanted

to get insights into user preferences by conducting focus group interviews. We will discuss our study structure in more detail in Section 3.2.2 "Study Structure".

To test our study, we conducted a pilot study with three participants and made minimal changes to our final study design. Since there were no major changes, we used the data from the pilot study for our analysis.

Users are not qualified designers, but there are benefits to considering user ideas

One fundamental concern about our study might be that users are usually not qualified designers. Black and Moran [1982] said that computer systems should not be designed by asking users what it should be like as they are not good designers.
However, researchers have also found that experts can not always accurately predict users' preferences. For example, Keleher et al. [2022] found that experts tend to overestimate users' ability to recognize manipulation. Similar to our study idea, users have tested and disliked software and then suggested better ideas, which the developers gained improved interfaces from[1]. Good et al. [1984] also argues that instead of adapting user behavior to interfaces, interfaces should be fit to users. They argue that untrained user behavior should be used to change a computer system to be intuitive and easily usable.
From these results, we conclude that there is a point to asking users for ideas. Especially when designing interfaces, however, we still have to consider their input with the caveat that users are not designers. While their ideas may be promising, the specific implementation could need changes.

3.2.1 Countermeasure-oriented Taxonomy

Existing taxonomies are not focused on countermeasures

While there are many existing taxonomies of deceptive patterns already, to our knowledge, none of them focus explicitly on countermeasures. For example, the ontology by Gray et al. [2024] has some deceptive patterns in the same category that may be more well-suited for different coun-

[1] `https://archive.org/details/byte-magazine-1983-02/page/n91/mode/1up`, *last accessed September 29, 2025*

termeasures, like *Privacy Maze* and *Intermediate Currency*, which they sort into the high-level pattern Sneaking. However, *Privacy Maze* works by adding steps and obstructing the user, while *Intermediate Currency* manipulates the available information to make the pricing harder for the user to understand. Since they work differently, it seems sensible that good countermeasures for them need to take different approaches.

This is why we constructed our own taxonomy, drawing inspiration from various existing taxonomies and focusing on how manipulative strategies might be countered.

We considered similar taxonomies and took inspiration from them

Bongard-Blanchy et al. [2021] identify the deceptive strategies coercive, nudging and deceptive as a consensus from other work, with different costs of resisting. This goes in a similar direction as our taxonomy by focusing on the underlying strategies, but we wanted to go into more detail and fully classify more patterns.
Another taxonomy that considers deceptive patterns similarly was published by Potel-Saville and Da Rocha [2023], where they pair deceptive patterns with corresponding fair patterns. While this is a helpful consideration, it is focused on fair patterns and not countermeasures and therefore not usable for our study.
Bösch et al. [2016] went a similar route by trying to understand the underlying concepts of deceptive patterns and collecting the strategies *Maximize, Publish, Centralize, Preserve, Obscure, Deny, Violate* and *Fake* that are the opposite of previously defined good privacy design strategies. This is aimed to analyze and understand deceptive patterns and how the manipulation works, as well as provide a starting point for developing countermeasures. However, this taxonomy is focused purely on privacy deceptive patterns and while there is some overlap with our taxonomy, it does not cover the same aspects.

Based on the lack of fitting taxonomies for what we needed and the goal of selecting a variety of deceptive patterns for our study, we created a new taxonomy.

Method

We collected and classified deceptive patterns into six categories

We collected deceptive patterns to classify through the ontology by Gray et al. [2024] as well as a few from Mildner's dark pattern cheatsheet[2] . After collecting a selection that covered most areas that are currently being researched, we started to sort them into clusters, focusing on how the deceptive patterns aimed to manipulate the user. We were inspired by the previously mentioned strategies by Bongard-Blanchy et al. [2021], but also considered other approaches to manipulation. Based on this, we decided on six categories into which all of our deceptive patterns could be sorted.

Categories

Our taxonomy's categories are MANIPULATED INFORMATION, OBSTRUCTION, COGNITIVE BIAS, PRESSURING, TAKING AWAY AGENCY and TEMPORAL

MANIPULATED INFORMATION: Deceptive Patterns that hide or manipulate the available information to trick the user. For example: *Trick Question, Language Inaccessibility, Manipulating Choice Architecture*.
OBSTRUCTION: Deceptive Patterns that make it hard for the user to do something or prevent it completely. For example: *Roach Motel, Privacy Maze*.
COGNITIVE BIAS: Deceptive Patterns that abuse human psychology, like heuristics. For example: *Bad Defaults*, *Infinite Scrolling*.
PRESSURING: Deceptive Patterns that pressure the user into doing something that they did not want to do or did not think about. For example: *Urgency*, *Confirmshaming*.
TAKING AWAY AGENCY: Deceptive Patterns that try to take away the user's choice completely. For example: *Sneak Into Basket*, *Forced Registration*, *Forced Communication or Disclosure*.
TEMPORAL: Multi-step or temporal patterns that may include multiple deceptive patterns over the course of an user interaction [Gray et al., 2025].

[2] `https://www.thomasmildner.me/darkpatterns.html`, *last accessed May 30, 2025*

3.2.2 Study Structure

The first part of our study was based on elicitation studies

Since our main goal was idea generation, we took inspiration from elicitation studies. Elicitation is a technique used to determine how to design intuitive gesture commands for user interactions with various devices and applications [Villarreal-Narvaez et al., 2020]. Similarly, our aim is to examine user preferences for how countermeasures against deceptive patterns should be designed.

We prioritized quantity over quality for the ideas

To generate as many ideas as possible, we took inspiration from a method called "Crazy 8's"[3] . The method is to set a timer for 8 minutes and aim to write down 8 ideas during that time. This helps participants come up with diverse ideas and focus on quantity rather than quality, which is supported by Liikkanen et al. [2009] and Kelly and Karau [1993]. We set a time limit of 15 minutes for the drawing rounds to include additional time for writing down explanations. In our pilot study, we separated this task, but our participants preferred doing it at the same time as drawing. While we asked participants to aim for 8 ideas, we did not put pressure on them to achieve this number.

We avoid already researched problems in our study

Alsebayel et al. [2024] describe capturing the context of deceptive patterns as a challenge of common methodology of user studies. To avoid the inexpressibility of static screenshots or video recordings, we implemented interactive prototypes on a locally hosted website. Using this, we were able to show our participants real-time interactions with deceptive website elements while we were explaining them, contributing to a better understanding of the manipulation.

Morris et al. [2014] explain the problem of legacy bias, which describes the problem that users' proposals in elicitation studies are often biased by their prior experience with other interfaces. To combat this, they suggest the techniques production, priming and partners. We included all three in our study by having participants draw multiple countermeasure ideas (production), informing them about technical possibilities beforehand (priming) and running the study in groups of two to three participants (partners).

[3] `https://conceptboard.com/de/blog/crazy-8s-vorlage-brainstorming/`, *last accessed June 10, 2025*

For the second part, we utilized focus groups to investigate user preferences

The group setting also allowed us to run discussions in a focus group structure. As has been found by previous research [Gill et al., 2008], focus groups are useful in obtaining a deep understanding of participants' experiences and beliefs, which suits our aim of understanding user preferences. To conduct these interviews with good results and a pleasant atmosphere for the participants, we followed Gill et al. [2008] and assembled groups of participants that were comfortable with each other so they could openly discuss their opinions by often having participants in the same groups that already knew each other. Due to our strategy of convenience recruiting, this mostly happened naturally. We also aimed for a size of 3 participants per group and provided a quiet, comfortable location to avoid distractions. To further ensure comfort and allow all participants to express their opinions to the best of their abilities, we ran the entire study in German. During the study, the participants were provided with snacks and drinks, and afterwards, a 20€ Amazon[4] gift card was raffled between all participants that wanted to enter.
We recorded audio during all discussions to analyze the content later.

Demographic Data

We collected basic demographic data of age, gender and current occupation

Before beginning with the main part of the study, we presented the participants with an informed consent sheet and a questionnaire to collect demographic data and gauge preexisting technical and deceptive pattern knowledge. All documents utilized in our study, including the complete demographic data questionnaire, can be found in Appendix B "Questionnaires" in both German and English. The demographic data consisted of age, gender and current occupation, such as studying or working.

We tried to estimate our participants' technical knowledge

To estimate participants' technical skills and internet usage, we asked for their daily internet usage in hours and if they spend a lot of time on online shopping websites. Furthermore, we asked how capable they felt of using the internet, whether they cared about internet security and if they felt like they paid a lot of attention to security when using the

[4] `https://www.amazon.com/`, *last accessed September 28, 2025*

internet. Finally, to get a first peek into the participants' general satisfaction with their internet interactions, we asked whether they have problems achieving their goals with the given functions on a website.

We asked for participants' previous deceptive pattern knowledge and then provided a definition so everyone could answer the remaining questions

Then we wanted to estimate participants' deceptive pattern knowledge. For this, we asked whether they had known what dark or deceptive patterns were before the study and requested them to define the term in an open text field. On the second page, we first provided a short definition of deceptive patterns to allow participants to more accurately answer the following questions even if they had no prior knowledge. In this definition, we included a general definition of the term, where we defined deceptive patterns as "elements of user interfaces which are designed to manipulate the user's decision-making and affect their autonomy" (translated). This definition was inspired by Brignull [2023]; Gray et al. [2024] and Mathur et al. [2019]. Then we provided examples for categories of deceptive patterns to give the participants some idea of what the term entails but avoided priming them by not giving concrete examples. After this definition, we asked how often participants encountered deceptive patterns when using the internet and how susceptible they thought they were. Then we repeated both questions asking participants to estimate what other people close to them experience to cover both self-assessment and assessment of other people. For all questions except the daily internet usage and the definition of deceptive patterns, we used a five point Likert Scale, with 1 encoding the lowest value ("Completely disagree") and 5 being the highest ("Completely agree").

Procedure

Our study procedure started with demographic data and a short introduction into the topic

When starting the main part of the study, we gave the participants a short introduction into deceptive patterns and countermeasures. For deceptive patterns, we again provided them with a definition and the categories from Gray et al. [2024], and for countermeasures we went over the basic concepts of detection and possibilities of technical countermeasures, while purposely keeping everything vague.

Our goal was to give participants a sense of what is possible and some inspiration while avoiding bias by not showing specific countermeasures, as bias can significantly impact a study's results [Fitton et al., 2018].

Participants drew, discussed and ranked countermeasures for two deceptive patterns, and then discussed their general opinions in a final discussion round

Afterward, we ran two design rounds. During these, participants were presented with a deceptive pattern and shown through an interaction with it, where they could ask any questions about the deceptive pattern they had. They were then given 15 minutes to draw countermeasures and write short explanations. After that time, they were asked to present their ideas to each other and discuss what they liked and disliked, before being given three stickers each to mark their favorite drawings. This was done for two deceptive patterns, before we moved on to the final discussion, for which we conducted a semi-structured interview. For the final discussion, we varied between asking the following questions (translated):

- What do you generally want from countermeasures?
- Have you noticed any similarities between your favorites or your countermeasures in general?
- What was the biggest challenge for you when designing the countermeasures?
- Which countermeasures sound most effective to you?
- Which countermeasures sound to you like they could be easily transferred to other deceptive patterns?
- Did you have concerns that some countermeasures might be problematic or unethical?
- How do you think future new deceptive patterns for which there are no specific countermeasures could be handled?
- If you were to ignore any technical limitations, would you have any other ideas?
- What would be your ideal countermeasure?

Lastly, the participants were given a short final questionnaire (see Appendix B "Questionnaires") to write down

their opinions on a few general questions concerning countermeasures.

Chosen Patterns

We chose a broad selection of deceptive patterns from our taxonomy

When choosing deceptive patterns to include in the study, we chose two to three patterns from each of the categories from Section 3.2.1 "Countermeasure-oriented Taxonomy" to achieve a broad selection while also staying within reasonable bounds. In total, we chose 14 deceptive patterns. We focused on deceptive patterns that did not have many countermeasures yet and would be hard to counter with simple ideas like hiding the element.

From the category MANIPULATED INFORMATION, we chose the patterns *Hidden Costs* and *Feedforward Ambiguity*. *Hidden Costs* can not simply be removed, as the costs that are concealed are a required part of the transaction. *Feedforward Ambiguity* was interesting to us because its effectiveness depends on the user's expectations, which could make designing a blanket countermeasure tricky.

For OBSTRUCTION, we chose the patterns *Dead End* and *Privacy Maze*, which both often depend on what the user wants to reach, as well as *Forced Work*, which could be hard to just remove from a website. *Dead End* and *Privacy Maze* are also interesting as they have similar constraints as *Feedforward Ambiguity*, which is why we wanted to compare the countermeasures for these patterns.

Another pattern that depends on what the user actually wants and that can also take different forms is *Bad Defaults* from the COGNITIVE BIAS cluster, as well as *Choice Overload* and *Infinite Scrolling*. *Choice Overload* would not profit from countermeasures that alert the user or give an explanation, as this would add even more visual clutter, but taking away some of the choices would limit the user's autonomy. For *Infinite Scrolling*, it could be interesting to compare user ideas to existing literature on countermeasures, for example Meinhardt et al. [2025].

For PRESSURING, we chose *Nagging* with a similar reasoning to *Choice Overload*, and *Confirmshaming* as a countermeasure specific to *Personalization* and *Emotional Manipulation* would be interesting.

For TAKING AWAY AGENCY, we chose *Forced Registration* because it can not simply be hidden as it is blocking something the user wants to access. Additionally, we chose *Sneak Into Basket* to compare it to *Hidden Costs*, because both are trying to sneak costs past the user, but one can be removed and the other cannot, and they occur in different steps of the process.

Lastly, we wanted to consider the new TEMPORAL pattern example that was introduced by Gray et al. [2025] as temporality and the interplay of multiple patterns increase the complexity of the manipulation and therefore the requirements for the countermeasures. For a second option, we created a new combination of patterns. In this fictional online shopping interaction, we included the patterns *Sneak Into Basket*, *Urgency*, *Personalization*, *Emotional Manipulation*, *Confirmshaming*, *Forced Registration*, *False Hierarchy*, *Hidden Costs* and *Bad Defaults*.

We created an interactive prototype to present the patterns to the participants

To present these patterns to the participants, we created a website prototype with a separate, fully interactive example for each of them. The full prototype can be found in Appendix A "Deceptive Pattern Definitions, Taxonomy and Examples".

3.2.3 Ethical Considerations

Per the ethical guidelines of the responsible institution, our study did not require an ethics review

Since we worked with manipulative design, we considered requesting an ethics review from our institution's responsible body. However, per the ethical guidelines of our institution, this was not necessary as there was no risk of harm and no manipulation of the participants.

3.2.4 Data Analysis

We analyzed the data using thematic analysis and an inductive coding approach in two rounds

We analyzed each part of the study individually. To transcribe the audio recordings, we used a locally hosted AI transcription tool[5] . We used Microsoft Excel[6] for descriptive statistics about the demographic data and for creating visuals.

Since the majority of our data was qualitative, we analyzed it using thematic analysis [Braun and Clarke, 2006]. We followed the six steps Braun and Clarke [2006] described: familiarizing with the data, generating initial codes, searching for themes, reviewing and naming themes and finally reporting the results. For generating the initial codes, we also used Burnard et al.'s inductive coding approach. For this, we roughly followed their four stages in two coding rounds: in the first one, we came up with the codes and aggregated them, and in the second round, we went through our data again and coded everything according to our codebook. It is important to note that our codes were not mutually exclusive, as often multiple different aspects were utilized in the same design. For the qualitative coding and analysis, we used the software MAXQDA[7] . It provides various features for coding, organizing data and analyzing the codes and connections. We also utilized its focus group options to pay attention to the unique nature of focus group interview data. As Gill et al. [2008] argue, focus group discussions have to be considered differently than other qualitative data because of their interactive nature.

[5] `https://git.rwth-aachen.de/i10/research/local-research-transcriber-python`, *last accessed 28.09.2025*

[6] `https://www.microsoft.com/en-us/microsoft-365/excel`, *last accessed September 19, 2025*

[7] `https://www.maxqda.com/`, *last accessed September 19, 2025*

3.3 Results

In this section, we will present our study's results. We translated all direct quotes from German to English.

3.3.1 Demographic Data

We had 18 participants with an average age of 22 and an even distribution of genders. All of them were students in technical subjects

Due to some cancellations, we ended up with 18 participants in total. 50% of participants were female, and the other half identified as male. The participants were aged between 20 and 28 (M = 22.39, SD = 1.98). In total, all the participants were university students and three additionally reported a student job as their current occupation. 66% of them were computer science bachelor students, while the rest were computer science master, mechanical engineering or civil engineering students.

All participants had a high internet usage

In terms of daily internet usage, 61% estimated using the internet for more than 5 hours a day, while the remaining participants put down 3 to 5 hours as their answer. The answers for "I spend a lot of time on online shopping websites" were balanced (M = 2.5, SD: 1.3). All participants claimed to feel capable when using the internet, with all values selected being either 4 or 5 (M = 4.56, SD: 0.5). Most participants claimed that internet security is important to them (M = 4.22, SD = 0.92), but all except one rated their habit of paying attention to it equally or lower (M = 3.67, SD = 0.82). When asked whether they rarely had problems achieving their goal on websites, participants leaned towards not having problems but were rather balanced (M = 3.11, SD = 1.05).

Deceptive pattern knowledge was balanced but leaned towards high knowledge

For deceptive pattern knowledge, we first asked participants to rate their previous knowledge. There were selections between 1 and 5 (M = 3.67, SD = 1.37), meaning we had a balanced participant grouped that leaned towards having more knowledge. For the definitions, the two participants that claimed no previous knowledge did not answer. The other participants mentioned manipulation or nudging (13/16), disadvantages for the user (6/16), unde-

sired results (5/16) and the company profiting from this (5/16). Most answers contained multiple aspects, and only one answer was "wrong" in the sense that it defined deceptive patterns as users' behavioral patterns without mentioning manipulative design at all.

3.3.2 Drawings

In total, the 14 design rounds resulted in 179 countermeasure drawings, split between the patterns as seen in Table 3.1.

We investigated 14 deceptive patterns and received 179 countermeasure drawings

Pattern	Participants	Drawings
Hidden Costs	3	13
Feedforward Ambiguity	2	16
Forced Work	3	13
Dead End	3	9
Privacy Maze	3	11
Infinite Scrolling	3	24
Bad Defaults	2	12
Choice Overload	2	9
Confirmshaming	2	6
Nagging	2	10
Sneak Into Basket	3	13
Forced Registration	2	11
Temporal	3	14
Temporal 2	3	18

Table 3.1: All patterns, the number of participants that designed countermeasures for them and the total amount of drawings. This allows us to see which patterns received a variety of designs and which had less.

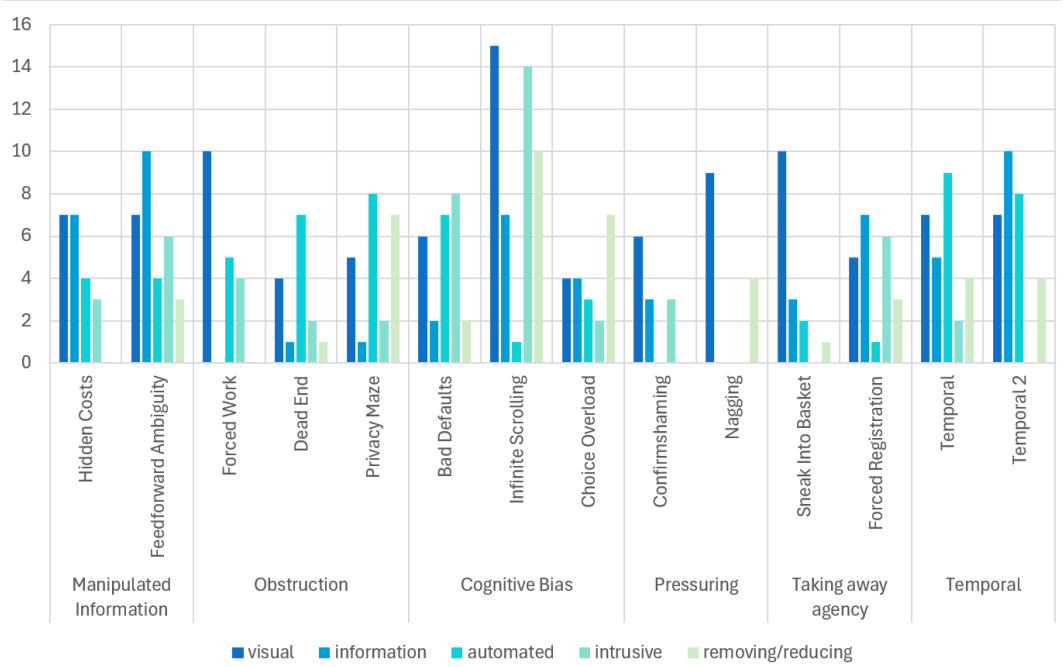

Figure 3.2: The top level codes and how often they were given for each pattern. Multiple codes could be given for the same countermeasure design. This allows us to see which codes were most represented for each pattern.

In this section, we will list the most popular designs suggested for each pattern, as well as how often codes were used, which combinations of codes were most popular and in which form the codes occurred. We will also mention which points participants additionally discussed when presenting their designs to each other. A full overview of all codes used during the qualitative analysis can be found in Appendix C "Codebook".

Deceptive Patterns

The countermeasures for *Hidden Costs* were focused on giving the user more information about the costs

MANIPULATED INFORMATION: For *Hidden Costs*, there were four countermeasure designs that received stars during the rating. Displaying all additional costs in the cart before checkout was suggested multiple times and received one star once and three stars once. Another idea was to display the additional costs earlier during the payment, and additionally warning the users of a violation of the law if it

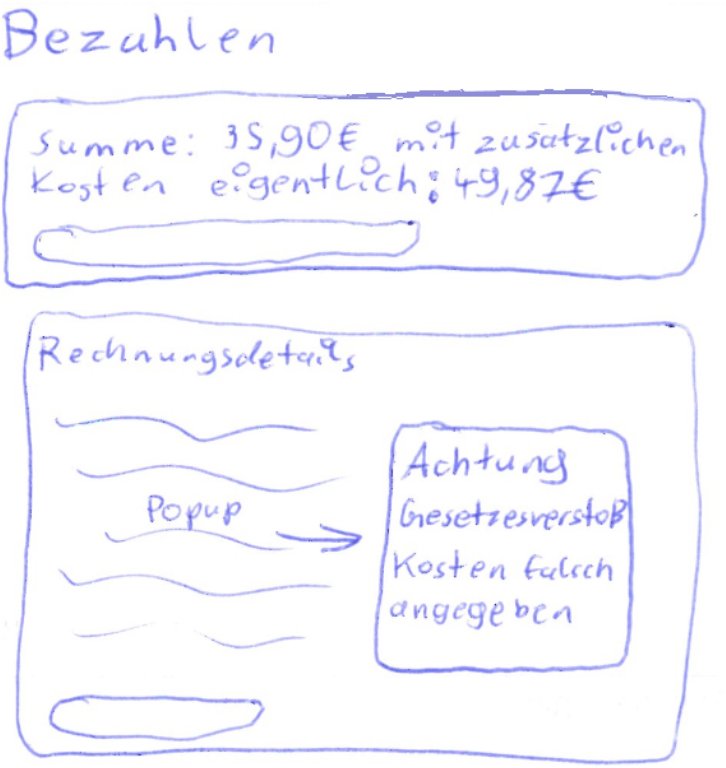

Figure 3.3: This countermeasure for *Hidden Costs* displays the hidden costs early in the process and warns the user about violations of the law if they occur.

was actually illegal to only add the costs at the very end (see Figure 3.3). This idea received two stars. Lastly, the second idea with three stars was the suggestion to add the additional costs to the cost of the product even before adding them to the cart, so the user immediately knows what the real price of their purchase would be.
The most common codes were “popup”, “inform about manipulation”, “highlight”, “visually display/modify”, “additional information (for the page itself)” and “shortcut/skip steps”.
When discussing their designs, participants mentioned not wanting generic popups because they would just be ignored after the second time. They also suggested working with color and visually highlighting relevant information. As an example where they liked the execution, they men-

tioned the online reselling platform Vinted[8] , where the additional costs for the platform's buyer protection are displayed right under the price of the product and therefore immediately obvious.

Feedforward Ambiguity's countermeasures were focused on explaining consequences, automatically rerouting the link or changing the structure of the interaction

Feedforward Ambiguity had four winning countermeasure designs as well. Rated with one star each were a popup explaining the manipulation or consequences, redirecting the click onto the supposedly intended link and blocking the interaction from appearing if not necessary or automatically denying it if possible. Rated with three stars, with one participant giving it two stars, was changing the structure of the window and marking the suggested action.
The most present codes were "popup", "rephrase", "autofill/-run", "visually display/modify", "solves similar problem" and "inform about consequences".
During the discussion, one participant commented on wanting to know when an extension does something automatically and what it did because it would give them a bad feeling otherwise. The participants also discussed whether they liked automation, as it was giving up control about what happened. They came to the conclusion that it would be better for some user groups than for others, naming the example of older users. When discussing whether they liked popups or not, one participant mentioned that in their countermeasure designs, when they included popups, they did not mean popups in the traditional sense but rather as information that unfolds when the user hovers over it.

Some countermeasures for *Forced Work* tried to skip the waiting time entirely and some tried to entertain the user during it

OBSTRUCTION: For *Forced Work*, the countermeasure ideas can be sorted into two categories. The first one are ideas that try to get rid of the manipulation by preventing it through technical measures. One such idea is an extension that pre-loads all sub-pages of a website and when the user actually clicks on a page, the waiting time is already over. Another would be to modify the system clock to skip the countdown. Both of these were rated with one star. An idea rated with two stars skips the waiting page by putting the intended link directly onto the button that would normally lead to the waiting page.
The second category is ideas that overlay the advertisement and pass the time with something else so the user is enter-

[8] `https://www.vinted.com/`, *last accessed September 28, 2025*

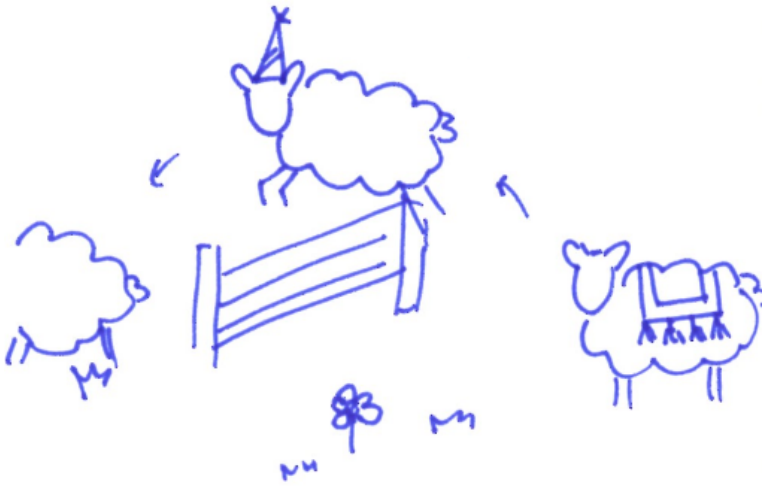

Figure 3.4: The winning countermeasure for *Forced Work* covers the advertisement with little sheep to entertain the user during the waiting time.

tained during the waiting time. Rated with two stars was the idea to display newspaper articles so the user can spend their time reading something useful, and rated with three stars was the idea to have little sheep in cute outfits that count down the waiting time, as seen in Figure 3.4.
The most common codes were "strike out/cover manipulation" and "entertainment".
When discussing the countermeasure ideas, participants were divided whether this is a pattern that always needs to be removed. One participant brought up the example that small editorial offices that provide good journalism have to pay their bills somehow, and that they do not want to take money away from that. Another point a participant made was that they do not want to be distracted by a countermeasure like something that would open a different page because they would have a hard time switching back to the task. However, they said something like the little sheep would be great because it would be something that passes a short wait without distracting the user.

For *Dead End*, the participants focused on ideas that gave the users the page they wanted to access or set all settings automatically

Dead End had two countermeasure designs that warned the user when a page was not found, which received one star each. One of them would also offer an alternative link to save the user the time of searching for the correct one on their own. The last one star idea was to have all settings of the page compiled into one big custom page, which might be chaotic but would contain all possible settings. The three star ideas were a plugin that automatically adjust every website's settings according to the user's pre-set global preferences, and an extension that replaces the inactive link with the correct one automatically after searching for pages with similar contents to what the user wanted.
The codes that occurred in most solutions were "autofill/-run" and "shortcut/skip steps".
While discussing their ideas, the participants raised concerns about replacing the link without telling the user and not trusting an extension that sets settings globally to work properly, even though they thought it would be great.

Privacy Maze had ideas that offered shortcuts, visually displayed paths or reduced the user's confusion

For *Privacy Maze*, the ideas were mostly concentrated into the codes "shortcut/skip steps", "visually display/modify" and "reduction".
The ideas that won stars also represent these codes: There were five ideas with one star, the first one was the computer having pre-calculated shortcuts for different settings, which would automatically be followed while showing all steps when the user chose one of them. The second one was a similar extension that provides links for pages that are often used like privacy settings, canceling a subscription etc. Another idea was to have a hovercast which shows you the next page when you hover over a link. The next idea was to have a "Wikihow" with tutorials on how to reach everything for every website, and the last one was to display all "Deny" buttons of the whole website on one page, so the user can choose directly. For two stars, the first idea was to have a popup in the beginning, which asks the user about relevant settings and then sets them automatically according to the user's preference. The second one was a search bar combined with an AI that finds the relevant pages for the user's search and returns them.
The idea of displaying all possible paths in the settings as a mind map or tree structure was suggested by all three participants but did not receive any stars.

When rating the countermeasures, one participant said that they chose their favorite because it did not require any additional text input from their side.

COGNITIVE BIAS: The first pattern from the COGNITIVE BIAS category was *Bad Defaults*, which was presented to a group with two participants. Two of the drawings included automatically deselecting "bad" and selecting "good" options. The one that did only that received one star, while the second one additionally marked the "good" and "bad" options in colors to nudge the user. The second idea that received one star was spatially sorting all fields by topic to make getting an overview easier. The last idea received two stars and was a "reset" button that removed all preselections.

Bad Defaults had mostly ideas that de-selected all options and marked which options were good or recommended

The most commonly found codes were "reverse manipulation", "autofill/-run", "shortcut/skip steps" and "visually display/modify".
During the discussion, P10 placed emphasis on their countermeasures not deciding what options were "good" or "bad" and acting accordingly, but rather neutrally determining which options were strictly necessary to continue and work with that instead. They argued that this would be much simpler and require less trust in the program. During the discussion, the participants also had additional ideas that went in a more entertaining direction, such as themed music warning the user of bad choices or a plugin which pulls the user's mouse away from "bad" options.

Choice Overload was another pattern in a group with two participants. They had three winning countermeasures with two stars each. The first one was a decision tree to allow the user to make a choice appropriate for their circumstances, with an added table with explanations for each option at the end. The second idea was to display all options in a table with the added information of the actual percentage of users that use each option. The last idea was an input field where the user could freely specify what was important to them, which would automatically be applied to every website.

The countermeasures for *Choice Overload* were focused on reducing the overload and helping the user make a decision

The most common codes were "spatial change", "reduction" and "additional information".

Figure 3.5: The winning countermeasure idea for *Infinite Scrolling* received four stars. The idea was to reduce the website's quality to discourage the user from scrolling.

Infinite Scrolling had the only four star countermeasure

For *Infinite Scrolling*, there was one countermeasure with four stars, as seen in Figure 3.5. The idea was for the website to get worse, for example through increased lag or reduced quality and brightness the longer the user scrolls to discourage them from scrolling. Limiting the scroll bar's size to a certain size and then not loading any further posts received two stars. Three ideas received one star: a reminder after a certain number of posts of how many posts the user has seen, the app or website closing itself, and the app or website disappearing and being blocked until the user has spent a certain amount of time away from their phone or doing something else.

There was a diverse number of codes strongly present for these countermeasures. The most common ones were "popup", "reverse manipulation", "remove feature", "friction", "inform about manipulation", "overlay", "visually display/modify" and "reduction".

Participants sorted their ideas into the categories awareness, blocking, and making scrolling less attractive

When discussing their ideas, participants categorized their ideas into three categories: awareness, being blocked completely or making it less attractive to keep scrolling. They also discussed that a lot of their designs were strong interferences in the website's functionality, so the user needed

to actively decide to use this countermeasure. At the same time, while they thought the more annoying ideas would be very effective, they would not want to use it themselves. When discussing what countermeasure would be most effective for themselves, all three participants had different opinions: P4 thought seeing how many posts they had already viewed would be enough for them, P5 said they would prefer a limit to the amount of posts they could see and P6 said for them the only thing that would work would be the app or website being blocked completely. One participant also commented on how this was "a difficult dark pattern to remove, because the users want to have it. They want to see as many posts as possible" (P5). They also discussed the idea of having a personalized assistant being "cute because it makes [the countermeasure] more personal" (P5). Another discussion topic was the idea of a starving animal that tries to emotionally manipulate the user to stop scrolling being a deceptive pattern in itself, which they said happens quickly with this pattern.

PRESSURING: The most popular countermeasure designs for *Confirmshaming* were rephrasing the shaming part by crossing it out very obviously and writing a reverse manipulative wording over it, as well as relocating all additional text that is not really needed into expandable info boxes. These received two stars each. Awarded with one star each were the ideas of naming the pattern with an overlay and offering a link to more information, as well as introducing an additional confirmation popup after the user chose the option they were shamed towards.

For *Confirmshaming*, the ideas focused on reversing the manipulation, removing or explaining it

The codes that were mostly given were "popup", "rephrase", "highlight", "overlay" and "strike out/cover manipulation".

About their idea of reversing the shaming manipulation, participants recognized that it was also manipulative but argued that "they balance each other out, and it's clear that the overlay is the extension. Because you have both, it's a compromise, like horseshoe theory?" (P11).

For *Nagging*, the most common code was "spatial change", and the other less common codes were "reduction" and "additional information (for the page itself)". The first design with two stars was outsourcing the information that

The countermeasures for *Nagging* were providing information less intrusively

is being brought up repeatedly and placing the link to this site in a less intrusive place. The other design with two stars was not having a popup, but rather a little arrow at the side of the page, which reveals the information when clicked. Both ideas rated with one star removed the popup and placed the information either at the top of the website or at the side without blocking the rest of the page.

The most popular countermeasure ideas for *Sneak Into Basket* warned the user about added costs

TAKING AWAY AGENCY: *Sneak Into Basket* had two countermeasure designs with three stars each. The first one was an AI clicking through the checkout process and warning the user of the additional costs. The second one worked similarly, tracking the real cart value and warning the user when inconsistencies arose. The other ideas were rated with one star each. Two of these were visual changes, the first one highlighting the option of removing things in the basket and the second one making the notification about the added costs be the same size as everything else so it is not overlooked as easily. The last idea was an extension that automatically removes everything the user did not add to their basket.
The most used codes were "highlight" and "additional information (for the page itself)".
When discussing their ideas, one participant said that they did not even notice that there was an option to remove the automatically added things from their basket at first, which would make them think they did not have the ability to opt out even if they noticed the deceptive pattern. Another participant suggested a reporting system for websites that use deceptive patterns, but also raised concerns about users not noticing "as people apparently don't even notice the HTTPS logo, so how would this actually work?" (P18).

For *Forced Registration*, approaches were informing the user as early as possible or making the registration voluntary

Forced Registration's most common codes were "popup" and "overlay" as well as "inform about manipulation" and "inform about consequences".
The winning ideas with one star were warning the user about the upcoming forced registration before opening the website, and providing the blocked content without registering, but telling the user what happened. Rated with two stars each were the idea to display the information about the pattern at the very start of the website, and making the registration voluntary by giving a "No" option which

would still allow the user to see the content.
During the discussion, one participant brought up the additional idea of having an extension that generates a disposable account to work around the registration without disclosing actual user data. This was also suggested to counter the *Forced Registration* aspect of the second Temporal variant. One aspect that both participants liked strongly was placing the countermeasure before the actual manipulation and interesting content so that the "hook" was less strong.

For both TEMPORAL variants, participants wanted to reduce the number of steps, remove individual deceptive patterns or to skip the entire process through automation

TEMPORAL: For TEMPORAL, we constructed two similar examples. One idea between both groups received three stars: adding an option on the first page that allowed the user to skip the rest of the process by automatically completing it for them, but also allowed them to go through the process on their own. The same idea by different participants also received one star and two stars, with the addition of removing all patterns from the process should the user choose to go through it, and one star by itself. Multiple participants also suggested restructuring the information to remove all manipulation and condensing the process to a single page, which received one and two stars. Three ideas were based on giving the user more information: The first one received one star and was an assistant that provided information from later in the process to the user. One of the other two rephrased information and removed unnecessary steps while also warning the user about the manipulation, while the other displayed how many steps and deceptive patterns were still ahead of the user. Both of these received two stars. The last idea with one star was a browser extension that creates and manages throwaway accounts so the user can circumvent patterns like *Forced Registration* but still profit from potential benefits such as discounts. Finally, rated with two stars, one participant suggested an assistant that should work through the process independently and provide a report of what they did and encountered at the end. Since the patterns are quite similar, most of the ideas could be applied to either variant.
The most highly represented codes were "inform about manipulation", "inform about consequences", "autofill/-run", "shortcut/skip steps", "visually display/modify", and "additional information (for the page itself)".
During the discussion in one of the two groups, the partic-

ipants categorized their favorite ideas into putting everything onto the same page and being navigated through the process by AI. One participant said about the first variant that "the whole thing is far too confusing for me, which means the only option I see is to hide things rather than add things, because that would just make it even more chaotic" (P2). They also argued that when doing something automatically, a report at the end is very important to them so they can catch potential mistakes. One participant preferred solutions that finished the process quickly because they're "trying to cancel a subscription I obviously don't like, so I'm fine with finding the button immediately and not having to deal with it at all. I have a problem, I want a solution and I don't care about the rest, as long as it does what I want it to" (P2).
There were also some differences between the two variants. As we can see in Figure 3.2, the second variant had a strong focus on "information", while for the first one, "automated" was the most common code. Another key difference is that the first one had some "intrusive" countermeasures, while the second one did not.

Codes

Most codes used for the drawings fell into the categories "information", "automated", "visual", "intrusive" and "removing/reducing"

Overall, most of the codes used for the drawings could be sorted into the categories of "information" as well as "automated", "visual", "intrusive" and "removing/reducing" countermeasures. The most used subcodes (>25 usages) were "popup", "inform about manipulation", "autofill/-run", "shortcut/skip steps", "spatial change", "visually display/modify", "reduction" and "additional information (for the page itself)". Detailed frequencies can be seen in Figure 3.6 or Appendix C "Codebook".

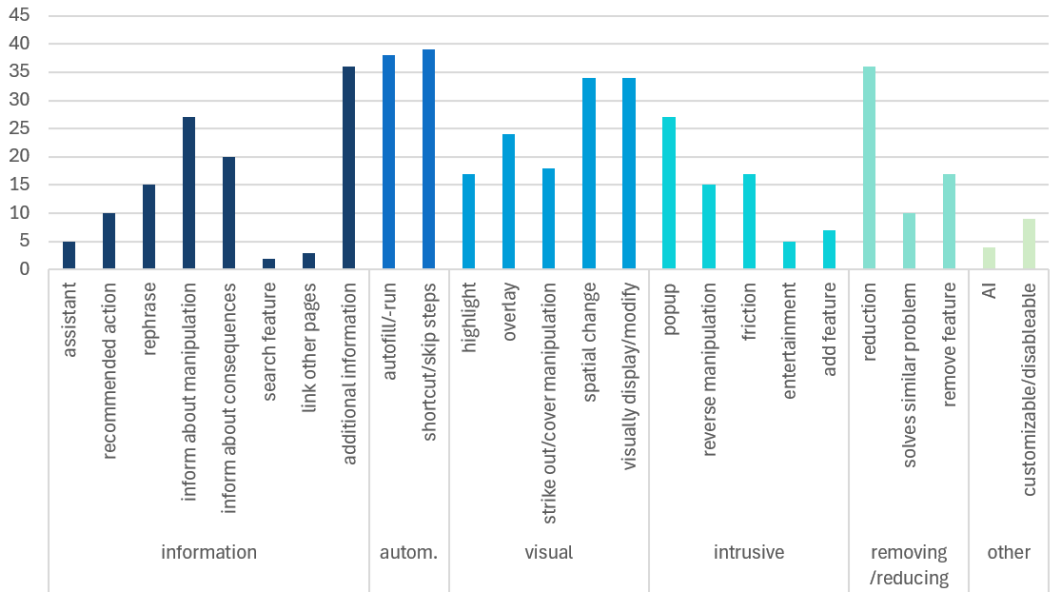

Figure 3.6: All codes for countermeasure design characteristics and their frequencies. This shows how often each individual code was used and which codes were most common.

Some codes were combined very frequently

Most designs contained multiple codes, resulting in some prominent code combinations. The most popular ones were "autofill/-run + shortcut/skip steps", "popup + friction" and "popup + inform about manipulation". "remove feature" was often combined with "autofill/-run" or "reduction". Further combinations that happened multiple times were "autofill/-run + customizable/disableable" and "spatial change + reduction".

3.3.3 Discussions

During the design rounds, there were some additional discussion points that were not directly related to the countermeasure drawings, which is what we will evaluate here. Afterward, we will look at the final questionnaire answers and discussion points.

Design Rounds

Participants were split whether some deceptive patterns were okay to keep

One topic that sparked discussion during the *Forced Work* discussion was whether all deceptive patterns need to be removed, or whether sometimes something like paying for a service is the better solution. While one participant argued that paying for something was exactly what the company wants to achieve by displaying advertisements and using deceptive patterns, another said that they were fine with paying for things they use daily. "You either pay with your time or with your money. I prefer paying with my money" (P15). They did however distinguish between paying for "a small editorial office's rent" (P15) and being forced to pay more than necessary because of corporate greed, with the latter being a reason for them to stop using a service or website completely. Similarly, a participant in another group posed that always removing all deceptive patterns was not the best solution as it could take options away from the user. They proposed the example of *Forced Registration* for a newsletter, which could also result in receiving a discount code, for which they argued an extension automatically creating a fake account would be better than blocking the registration prompt differently, so the user could still profit from the discount.

Participants did not want to be confused or distracted by countermeasures

Participants also discussed being distracted by countermeasures, which was something they generally wanted to avoid. They want something that takes away the manipulation but still keeps them on the site, so they do not forget to do the task.
Another topic mentioned multiple time was that chaotic or confusing countermeasures need explanations to work. If something offers a lot of additional information that might not be immediately comprehensible, it should also highlight the relevant parts for the user's current situation to prevent them from being overwhelmed. On the other hand, some participants raised concerns about countermeasures being too inconspicuous and therefore not as effective because they are overlooked easily. They said that countermeasures need to be prominent or make their options more obvious, as otherwise they would not even know they have a chance to counter the deceptive pattern.

The most effective countermeasures could be annoying to use

In terms of practicality, participants discussed that sometimes the most effective countermeasures would also be very annoying and that they themselves would not want to use them. An example is the winning countermeasure for *Infinite Scrolling*.
They also raised the concern that some countermeasures work better on some devices. For example, on a computer screen a visual assistant may be fine, but on a phone it would take up too much space.

Other discussion topics include a report system, error rates, needing awareness to profit from countermeasures and timing

One participant suggested a report system as one of their countermeasure ideas, which was originally received well. However, they then argued that a system based on user inputs was prone to some people adding links leading to dangerous websites or wrong information.
Multiple participants in different groups discussed how tolerable mistakes made by the countermeasure were. They came to the conclusion that if the countermeasure did not notify them of the changes it made, they would always worry that it did something wrong. In a similar vein, another participant suggested that if the countermeasure could not handle a deceptive pattern for whatever reason, it would need to notice on its own and react accordingly.
One participant suggested having a website that raises awareness and provides education as a countermeasure. Another participant argued that to benefit from something like this, users already need awareness that deceptive patterns are a problem and that solutions for it exist, which many do not have.
Lastly, the point of timing was also brought up multiple times. Information about the pattern or consequences of actions should be added as early as possible to give the user time to prepare and acknowledge the manipulation before it has already happened.

Final Questionnaire

What is important to you when it comes to countermeasures in general?

Participants valued transparency, autonomy, simplicity, low effort and a pleasant user experience

The aspects that were mentioned the most were transparency and autonomy, with the participants wanting information and control over the applied countermeasures, nothing to be hidden, the ability to see the original website as well as the option to get an explanation of what happened. They also wanted simplicity and low complexity as well as no effort for the user and preferably a set-and-forget solution. In terms of user experience, they wanted the countermeasures to not be too intrusive and to keep the website functional and attractive. A few users wanted entertainment to increase likability and approachability.
Some infrequently mentioned aspects were visually reducing clutter or removing colors, displaying the legal framework and having reoccurring website elements designed the same everywhere. Other than that, participants wanted information, customizability, early timing and few popups except if they offer the option to end something immediately. Some participants placed a lot of importance on the admission that mistakes might happen, that they would rather have a countermeasure do too little than too much, and that they do not want everything removed completely so they can be prepared for when the countermeasure may not work. One participant wrote that deceptive patterns are only part of an underlying problem, for example companies being able to profit off selling user data.

Did you notice similarities between your favorite countermeasures?

The biggest similarities between favorite countermeasures were simplicity and ease of use

For this question, 13 out of 18 participants answered with some variation of simplicity and ease of use. Other aspects that were mentioned were that the user experience was efficient, not annoying, and improved by additional features and entertainment. Additional observations include high information content, explanations, displaying violations of the law, not patronizing and being applicable to different websites. Some participants mentioned that their favorites acted visually, removing colors from the website or highlighting the countermeasure and hiding unneeded options.

What would your ideal countermeasure look like?

There were a lot of requirements for the perfect countermeasure

For their ideal countermeasure, participants wanted something that made it obvious that it changed something and gave them the ability to undo the change. Some participants rather wanted it to be invisible and not bother them. They also wanted it to be clear, easy to use and integrated into their browser. In some discussions, they mentioned wanting a set-and-forget solution or to not deal with it at all, while still keeping their user experience the same. Some participants mentioned achieving this by having a browser extension where you can customize the countermeasure once and then have them applied to every website as best as possible. Generally, 10 participants mentioned wanting information and highlights of important things, as well as explanations and recommended actions. Another aspect that was mentioned again was customizability of which website to apply which countermeasure to. To some participants, it was also very important to have standardization of all legally binding fields and that they could always find all important information in the same place.

How could countermeasures be designed to deal with future deceptive patterns before there are specific countermeasures for them?

Future deceptive patterns could by countered by education, AI or visual design changes

When asked for ideas for countermeasures against new deceptive patterns, most participants suggested informing about the pattern in some way. Ideas included highlighting the pattern with or without explanation, as well as training users in dealing with deceptive patterns so they were able to transfer their knowledge to new patterns on their own.
Here, suggestions also included AI, for example to be trained by users and reviewed by experts, to learn existing countermeasures generally and come up with new ones or to browse the web human-like to find new deceptive patterns. Another idea similar to training through user reports was a report system, for example in form of a website that collects patterns or websites that contain them. The extension could then warn the user when they enter a website that is known to use deceptive patterns.
Some more visual ideas include making videos and other external content able to be hidden or grayed out, or generally exporting all important information to your own formatting.

Suggestions for finding these new patterns and dealing with them very generally were also offered, including concentrating on fundamental characteristics of deceptive and fair design instead of specific countermeasures, paying attention to certain keywords such as "Deny" and recognizing reoccurring patterns.

Additional comments:
A few participants provided additional comments. One participant suggested a cooperation with Trusted Shops[9] , which is a platform protecting user purchases on cooperating online shops and provides a certification for websites to display to show their trustworthiness. Another referred to PayPal's[10] standardized checkout page for every website where you can pay with it and suggested making this the standard not just for PayPal but for every checkout page.
One participant placed importance on adjusting the countermeasure to the user and gave the example of giving children more extreme countermeasures.
Lastly, one participant commented that technical countermeasures can only be a temporary emergency solution and that fair design has to be legally required to solve the problem of deceptive patterns.

Final Discussion

During the final discussion, some points came up in multiple groups.

Popups were a controversial topic

One popular topic were popups, about which there were strong opinions. Generally, participants did not want to be overwhelmed by them. One participant in particular did not want any popups at all, going as far as to say "if you give me one more popup, I will throw my computer out the window" (P2). Other participants argued similarly, saying that everything that does not immediately help the user end something is too much and will probably be ignored. Another participant claimed that you still have to give the user options and can not base everything around "the idiot who will click anything just to get rid of it" (P10).

[9] `https://www.trustedshops.com/`, *last accessed September 28, 2025*
[10] `https://www.paypal.com/`, *last accessed September 28, 2025*

Participants liked working visually and especially with color, as well as removing overload

Multiple groups discussed working with colors, mainly removing it to weaken the manipulation or making all options the same color. They said having most things in black and white instead of loud and manipulative colors would already help them. Someone also suggested highlighting what the countermeasure extension thinks is important or sensible in color after removing it from everything else.
Similarly, one participant highlighted that they liked designs that reduced the input the user had to process. They especially liked the example for *Forced Registration* that removed the "hook" of the article because "it's not something that imposes an additional burden, but rather takes something out" (P11).
Additional comments on the user experience were that some participants wanted it to stay the same, either for transparency or to have the choice to leave the website. Others preferred removal of all deceptive patterns and standardization of all relevant fields to streamline their user experience without manipulation. Mostly, they arrived at the conclusion that it should be customizable.

Customizability was wanted for both user groups and websites

Customizability also came up multiple times in the form of user groups. One participant distinguished between older generations, for which they said a simple display with no manipulation might be better, while younger people could deal with other countermeasures as they're more used to the internet. "I'm not going to try to teach my grandma about cookies now, but with children and young adults, it might be better to give them time to learn. Countermeasures should meet different requirements" (P9). Multiple groups also came to the conclusion that the countermeasures need to be accessible and intuitive for a broad target audience, rather than only focusing on people with a lot of technical knowledge.

Participants were unsure about the effectiveness of education

While many participants suggested some form of education, some also brought up the question whether education actually helps users resist deceptive patterns. They argued that, especially for new deceptive strategies, digital literacy and not trusting things on the internet is the only thing that can really help preemptively. Other participants strongly argued for technical countermeasures over education, saying things like "I know I can't psychologically defend my-

self against this after reading it" (P2). Other participants agreed that it would be better for them if the manipulation was removed completely and they were not confronted with it.

Participants were worried about the countermeasures making mistakes

Another topic of discussion was fault tolerance. Participants wanted their countermeasures to be as mistake free as possible. Some also said that they did not want the countermeasure to do anything silently and automatically, because they would be scared that it made a mistake without them knowing. Additionally, one participant said they would prefer "a removal or detection not to work than do too much" (P16).

There were concerns about AI usage, but also arguments that if used, it should be trained very generalized

As it is a currently popular topic, many participants brought up Artificial Intelligence (AI) in their designs or discussions. While it was often utilized, almost all participants raised concerns about environmental, copyright or privacy issues and were scared of hallucinations or other mistakes an AI might make. One participant argued that automating countermeasures, especially for future deceptive patterns, will have to rely on AI, for which they thought it was important to train it very generalized. "We can't tell it 'hey, there's False Hierarchy, which looks like this', etc. We rather should teach it the general nature of dark patterns, that they are manipulative. And if you teach it about their characteristics in general and the idea behind them, there may be a better chance of recognizing dark patterns" (P5).

Some participants were unsure whether all deceptive patterns need to be removed

For some examples, participants felt divided whether they actually wanted to remove the deceptive pattern completely and how. One consideration was not wanting to hinder the website's functionality, as for example a subscription is an important part of the site that a countermeasure should not just remove completely. Another participants found it immoral to remove patterns from certain websites, for example if they are providing an important service and need to e.g. show ads to pay their costs.

Bright patterns were another controversial topic

Another topic that participants had moral qualms about were bright patterns. Some countermeasure designs included manipulation towards the thing the user suppos-

edly wants. Multiple participants considered whether tricking the user for good was okay, as it still takes the user's agency away. One participant concluded that only "manipulation against one's own interests" (P9) was immoral.

Participants considered technical countermeasures not the ideal solution and deceptive patterns not the main problem that needs to be fixed

For some participants, technical countermeasures were not the ideal solution. Even though our study focused on technical solutions, participants brought up laws as an example of something that would be easier to fix the problem. They considered technical countermeasures to be more difficult because "it's always like an arms race" (P11). At the same time, participants acknowledged that some laws are already trying to regulate bad internet practices, but not very successfully yet.
Another problem one participant had was that they considered the root of the problem to be worse than deceptive patterns. They said that the underlying problem was not the design but rather the collecting and selling of data. They concluded that technical countermeasures are like "a band-aid on a laceration, but better than nothing" (P11).
When coming up with designs, participants also noted that they were already so used to deceptive patterns that their standards for websites had lowered and they did not care as much. One participant said they had already searched for solutions such as extensions that automatically deny cookies and were therefore limited in their creativity.

Chapter 4

Discussion

In the following, we will discuss our study's results and compare them with previous work, starting with the designs and then continuing with the questionnaire answers and discussions. We interpret their implications for countermeasure design. Finally, we will review our study's limitations.

4.1 Countermeasure Ideas

4.1.1 By Pattern

First, we will discuss the winning countermeasures and most represented codes by pattern.

Adding information or highlights to counter *Hidden Costs* is in line with existing literature

MANIPULATED INFORMATION: Both winning countermeasures for *Hidden Costs* had the additional costs that the user would normally be surprised by displayed earlier. This is in line with our expectations, as the easiest way to counter not being informed about upcoming costs is informing about them early. The prominence of "inform about manipulation" is in line with findings by Schäfer et al. [2024], where participants preferred the highlighting and explaining countermeasure for situations where there could be hidden costs. "visually display/modify" was very com-

mon because participants often highlighted the additional information of their countermeasure, the costs themselves or other aspects of the site to make them more noticeable.

Feedforward Ambiguity had mostly options that reduced the users confusion

For *Feedforward Ambiguity*, the winning countermeasure was to change the window's structure and mark the recommended action. Especially the common code "rephrase" makes sense to reduce some of the confusion of what the user's options do. Popups were used to provide the user with more information or give them the option to reverse their decision, also trying to reduce the confusion or at least help undo the action when the user realizes it was not what they wanted. To our knowledge, this idea is not something that previous research has covered.

Participants focused on overlaying the advertisements for *Forced Work* with entertainment to avoid technical problems

OBSTRUCTION: For *Forced Work*, the winning countermeasure was to overlay the advertisement with little sheep that counted down the waiting time. The most common codes "strike out/cover manipulation" and "entertainment" make sense, as the participants exclaimed not being sure what was technically feasible, and if their other ideas of skipping the waiting time through various means did not work, they wanted to find ways to pass the time better than watching an advertisement. To our knowledge, the aspect of entertainment in countermeasures has not been researched so far, so this could be interesting to look into further.

The ideas for *Dead End* support countermeasures investigated by existing research

Dead End had two winning countermeasures that worked very differently, but both contained the most used codes "autofill/-run" and "shortcut/skip steps". While the idea of automatically replacing the inactive link won, participants discussed whether automatically changing something without telling the user was okay. One participant said that it was important to tell the user if the countermeasure changed a link, as it would significantly influence their decision to keep using a website. This supports findings by Schäfer et al. [2024], who found that users do not want countermeasures to silently and automatically hide information, partially because it could make a website seem more trustworthy than it is. The second idea was a plugin similar to an idea proposed by Porcelli et al. [2024], who created a user support tool that lets user create a standard-

ized personal privacy policy. The policy is then automatically applied to every website by generating steps from the policy and applying them to cookie banners.

Privacy Maze had ideas that are in line with existing research

A similar idea was proposed for *Privacy Maze*, where the first time a user visited a site, they would receive some popups for relevant settings. Another winning design was having a search bar and an AI which searches for the relevant pages for the user's search and returns them. A related idea, "PriSEC", was proposed by Khandelwal et al. [2021], who suggested a browser extension that collects all privacy options and presents them in a searchable, centralized interface and enforces them automatically on user demand. Both ideas involve searching for and collecting relevant settings pages separate from the website, while the participant idea from our study is more focused on searching first and using AI to find something matching the search terms, while Khandelwal et al. [2021] focus on presenting all setting options first and then letting the user search through them. As we discussed in 2 "Related Work", this was found to be accurate and effective.
Interestingly, all three participants suggested displaying all paths through the privacy settings as a mind map or tree structure, but it did not win any stars. This may be due to the concerns about high complexity and lack of clarity. One participant countered this by adding a search bar and highlighting relevant paths, which is in line with the fair pattern "seamless path" that Potel-Saville and Da Rocha [2023] introduced as the counterpart to the deceptive strategy "maze".
The most commonly used codes were "shortcut/skip steps", "visually display/modify" and "reduction", which makes sense, as skipping steps reduces the confusion of running into a maze. Displaying the maze visually may also help provide the user with an overview, and when combined with highlighting relevant paths, which one participant placed great importance on, can also help them find their way faster. Lastly, "reduction" is fitting as it combines measures that can weaken the confusion that *Privacy Maze* builds on.

The countermeasures for *Bad Defaults* had ideas that neutralized the website or required some sort of judgment to mark recommended options

COGNITIVE BIAS: *Bad Defaults* had countermeasure ideas with varying degrees of intervention, which is reflected in the distribution of most common codes, which were "reverse manipulation", "autofill/-run", "shortcut/skip steps" and "visually display/modify". The first winning design was inserting a reset button to deselect all boxes, which is an option that gives the user a lot of autonomy by just adding the option of resetting the website to a neutral state. The second one was an extension that automatically deselected all "bad" options and marked the "good" and "bad" options in respective colors. This is more intrusive to the user experience as it actively makes changes to the website based on what the extension judges as good and bad options, and then further influences the user by marking the recommended options in a positive color.

Choice Overload had a surprising amount of options with "additional information

The countermeasure ideas for *Choice Overload* were mostly focused on "spatial change" and "reduction", which makes sense as restructuring the information and weakening the overload seem like obvious counters for this pattern, but also "additional information". This was surprising, as it seems counterintuitive to add more information to a situation where the user is already overwhelmed. King and Stephan [2021] also argue that giving the user more checkboxes or buttons does not solve the problem of overwhelming deceptive patterns.
The winning countermeasure of a decision tree makes sense when trying to reduce the overload by not presenting all options at once. The second idea was presenting all options in a table and adding the information of how many users actually use this option. Restructuring the options and giving additional information on how popular each one is seems like a good idea to help the user choose, however it might be precarious when considering the pattern Social Proof, which could also be used to manipulate users. Assuming that the data comes from the countermeasure and is correct, and considering that the participants said they would find this information interesting, this concern seems negligible. The last idea was similar to the designs for *Dead End* and *Privacy Maze*: the user gets an input field to generally enter what they want from e.g. a subscription, which is then applied to every page the user visits, automating the entire process of choosing an option. The participants were

cautious that this should only be applied to pages where the user actually wants to subscribe to something. To our knowledge, none of these ideas have been implemented yet.

The countermeasures for *Infinite Scrolling* support existing literature, but were also controversial among participants

While participants agreed that the winning countermeasure for *Infinite Scrolling* would be very effective, they also said that they would not want to use this extension themselves because it would ruin their user experience. This is a very interesting point, as it highlights that the most effective countermeasure might not always be what users actually want. This is important to consider because if users will not use a countermeasure, it does not matter how well it works.
The participants also said that this was a difficult pattern to come up with countermeasures for, as seeing many posts was something that users wanted. This highlights the importance of users actively choosing what and when to use countermeasures, as they can be a strong invasion into the user experience. The common codes "reverse manipulation" and "friction" are in line with findings by Meinhardt et al. [2025], who investigated interventions. They concluded that a multi-step approach or more severe interventions may be necessary when users are in bed or at home. Multi-step interventions fit with our participants' suggestions of their countermeasures acting stronger when more time passes. Our participants also commented on some of their ideas being too extreme. This might fit certain scenarios better than others, as Meinhardt et al. [2025] suggested. The other common codes were "remove feature" and "reduction" make sense, as they introduce additional barriers for the user to keep scrolling, such as reloading the page instead of just scrolling endlessly. Both adding additional barriers and making the website less pleasant to use are in line with the ways to demotivate immediate desires, in this case continuously scrolling, by Ozkaramanli et al. [2017].

The countermeasures for *Confirmshaming* introduced elements to make the user think about the manipulation or remove it

PRESSURING: The countermeasures for *Confirmshaming* were removing the manipulation but not completely hide any information from the user, and rewriting the shaming text by crossing it out and writing a reversely manipulative text over the top. This could be effective by making the user think about what they are reading and realize that they are

being manipulated. Both still leave the user's autonomy intact as they have all information, even though they also use the manipulative tactics of *Obstruction* and *Shaming*.

Nagging had countermeasures that changed it into a fair pattern

Nagging had one winning code, which was "spatial change". In most of their ideas, participants removed the reoccurring popup aspect of the pattern and replaced it by subtly placing the information somewhere else. This reflects the fair pattern "non-intrusive information" Potel-Saville and Da Rocha [2023] named as the counterpart to "push & pressure", which is the category that best describes *Nagging*.

Sneak Into Basket countermeasures were focused on informing the user

TAKING AWAY AGENCY: For *Sneak Into Basket*, participants clearly preferred countermeasures that used "highlight" and "additional information (for the page itself)" to warn the user of what is happening. Both winning countermeasures did this and reduce the possibility that a user might miss the item being added to their cart and therefore weaken the manipulation, which should be technically feasible.

For *Forced Registration*, there was some uncertainty about legality and technical options

Forced Registration had some ideas that tried to warn the user about the pattern before the website had a chance to "hook" them, and some that removed the forcing of the registration and made it optional instead. Both of these approaches had one winning countermeasure. If possible, participants preferred the second option, as they remarked that they wanted to read news articles without having to register. For a more technically feasible and legal option, participants proposed the first idea in various forms to weaken the pattern by placing the warning about it before the content that would catch the user's interest. These ideas have not been researched yet, as far as we know. Of course, piracy to avoid registering or paying for something is an existing concept, but also illegal. To our knowledge, the aspect of timing for countermeasures has not been researched yet.

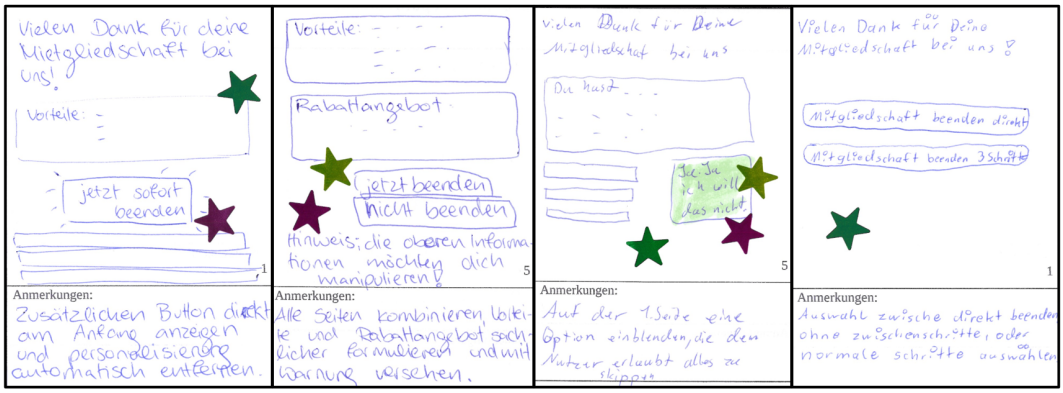

Figure 4.1: The most popular countermeasures for the first *Temporal* variant. All include an option to skip the entire process and immediately end the subscription.

The *Temporal* interaction was too complex for participants and they wanted to shorten or skip it

TEMPORAL: Across both *Temporal* pattern variants, there was one winning countermeasure: Adding a button on the first page of the interaction that would allow the user to skip everything and have it done automatically (see Figure 4.1). "shortcut/skip steps" was the most used code, further emphasizing that participants mainly wanted to find ways to shorten the interaction, allowing for less manipulation along the way. Gray et al. [2025] put the interplay and connection of the different patterns along the interaction as the main manipulative aspect of this kind of pattern, which would be reduced by reducing the number of steps a user has to take and therefore exposing them to less manipulation.

The codes that were most common for the suggested countermeasures mostly fall into the categories of information ("inform about manipulation", "inform about consequences", "additional information (for the page itself)") and automation ("autofill/-run", "shortcut/skip steps"), as well as "visually display/modify". Especially skipping steps or automating the process make sense, as one participant remarked finding the interface way too overwhelming and only seeing removing things as an option. Informing the user about the manipulation or the consequences was usually aimed at helping them through the process without missing anything and giving some overview of what was happening, which is also a way to support the user in their interaction. Since Gray et al. [2025] only recently brought up temporality, there are no specific countermeasures yet.

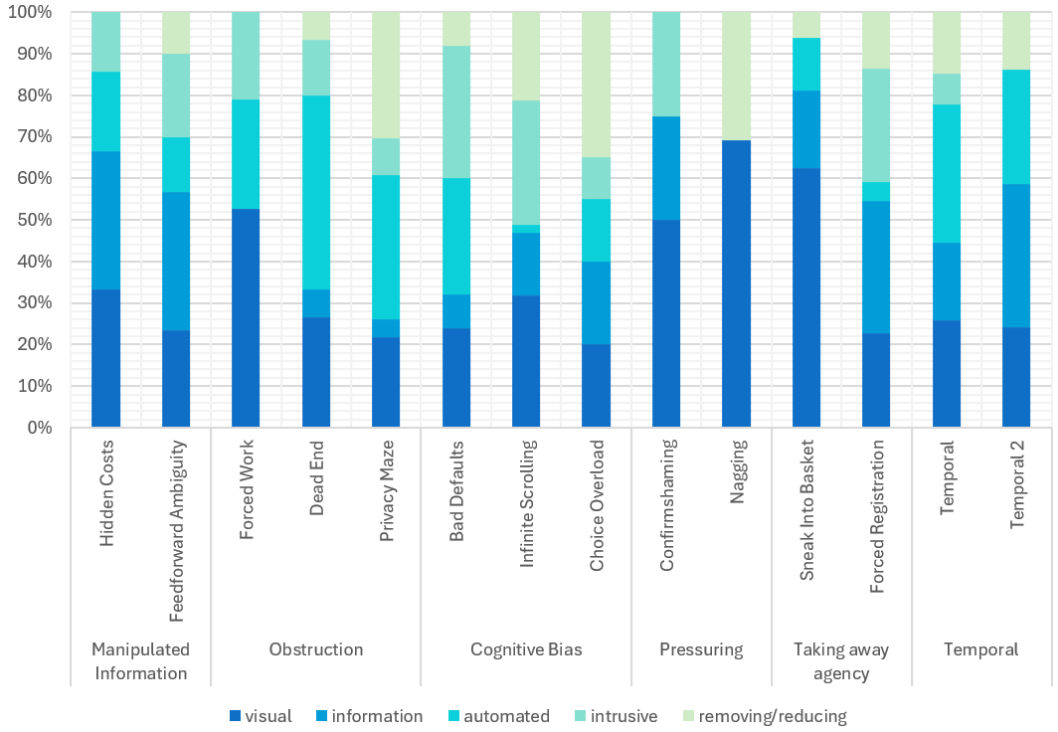

Figure 4.2: The top level codes and what percentage of given codes they were for each pattern. Multiple codes could be given for the same countermeasure design. This shows how often which kind of countermeasure was designed for each pattern in relation to all drawings for that pattern.

4.1.2 Similarities between Patterns and in Categories

There were similarities within deceptive pattern categories *Hidden Costs* and *Feedforward Ambiguity* had similar code distributions

In our deceptive pattern categories, there were some similarities.

For MANIPULATED INFORMATION, both *Hidden Costs* and *Feedforward Ambiguity* had "visually display/modify" as one of their strongest codes. Considering Figure 4.2, their top level code distribution also looks similar, the main difference being that *Feedforward Ambiguity* had some "removing/reducing", while *Hidden Costs* did not. The general similarities make sense and are in line with why we placed them in the same category, as making visual changes could highlight the concealed information in *Hidden Costs* and help understand the options in *Feedforward Ambiguity* better. Their differences also make sense, as *Feedforward Ambi-*

guity would profit more from a change in UX if it reduced the confusion the user faces, while *Hidden Costs* is already missing information.

The patterns for OBSTRUCTION had similar distributions

The patterns in the category OBSTRUCTION also have similar top level code distributions. Especially *Dead End* and *Privacy Maze* look very similar, while *Forced Work* had more focus on "visual" and in turn no "removing/reducing" or "information". *Dead End* and *Privacy Maze* are more similar to each other than to *Forced Work* as patterns, so these differences in the countermeasures make sense. Additionally, *Forced Work* having a lot of "visual" countermeasures is explained by the participants trying to counter it by overlaying it with something else to remove the manipulation, which is not an option for the other two patterns. It also makes sense that *Privacy Maze* has more "removing/reducing" than *Dead End*, as it is more confusing and overwhelming, while *Dead End* is already missing information or options.

There was more diversity in COGNITIVE BIAS

For COGNITIVE BIAS, the distributions differ a bit. As *Infinite Scrolling* is not really a pattern that can be dealt with by automating something, but rather visually or through changing the user experience, it makes sense that its countermeasures did not include automation, which was more prominent for the other two. For *Choice Overload*, it is also obvious that "removing/reducing" is sensible as the most common code category, as countermeasures for this pattern mostly need to reduce the overload to be effective.

PRESSURING and TAKING AWAY AGENCY had very different distributions in their patterns

In PRESSURING and TAKING AWAY AGENCY, there was little overlap, except that "visual" was very present for most patterns. This could mean that the patterns belong in different categories. To decide this, we would need to investigate more patterns from the categories, as two is a very small sample size.

There were some differences between both TEMPORAL variants, but overall they were very similar

Both TEMPORAL variants had similar amounts of "removing/reducing" and "visual". The amount of "information" is slightly higher for the second variant, while the first one had more "automated" and "intrusive". The first variant had a very confusing and overwhelming process, which explains why the participants wanted to automate parts of it. The second variant received a lot of new information: participants displayed how many steps were still ahead to give the user a sense of where they are in the process, added information about costs and about other potential sites to re-

duce the pressure on the user. This might be due to the fact that the first variant, the subscription canceling interaction, was something that could be completed automatically as the user would have a clear goal in mind. The second variant required more choices and input, which is why informing the user about different aspects of the interaction, such as the manipulation or consequences, might have been preferred by participants.

Looking at Figure 4.2, one can see similarities between the top level code distributions for some patterns, even ones that are not in the same category.

There was a surprising overlap between *Feedforward Ambiguity* and *Forced Registration*

Feedforward Ambiguity and *Forced Registration* both had "information" as their top code and similar distributions overall. This is surprising as they are fairly different patterns, with *Feedforward Ambiguity* utilizing confusion and *Forced Registration* relying on obstruction. Considering this, "information" makes more sense for *Feedforward Ambiguity* than for *Forced Registration*, as it does not counter the obstructing aspect of the pattern. Looking at the individual countermeasures, however, we can see that some of them contained "inform about consequences", where the participants tried to warn the user about the *Forced Registration* earlier to prepare them.

Dead End and *Privacy Maze* were expected to be similar, but *Bad Defaults* and *Temporal* are surprising

Dead End, *Privacy Maze*, *Bad Defaults* and *Temporal* share "automated" as their top code and a generally similar distributions. Overall, *Dead End* and *Privacy Maze* are very similar patterns and in the same category in our taxonomy. *Bad Defaults* is surprising, as it does not share any similarities with the other two patterns at first glance as it works through the user's assumption that the default option is the best one, while the other two share the strategy of confusing and obstructing the user. *Temporal* did not contain any of these three patterns, but was very similar in adding steps to confuse the user and giving a lot of options, which is why it makes sense that the countermeasures went in a similar direction.

We chose some patterns for our study specifically because we wanted to compare their countermeasures.
The first such pair was *Hidden Costs* and *Sneak Into Basket*. There were a lot of similarities between the two, starting with the countermeasure designs. For both patterns, par-

ticipants suggested warning the user about the additional costs ahead of time, or simply showing them earlier. A point that was discussed for both was visually highlighting the costs, information, or removal options to make sure the user notices the important things. Both had "highlight" and "additional information" as their most common codes, which fits the discussion and winning countermeasure ideas. It also makes sense, as the patterns withhold or conceal important information. Codes that were present a little for both patterns were "inform about consequences", "overlay", "spatial change" and "visually display/modify", which seem plausible for the aforementioned reason as well. There were some differences: *Sneak Into Basket* also contained the codes "autofill/-run", "AI" and "reduction" a lot, which fit the pattern better than *Hidden Costs*, for example something that was automatically added to the website could be automatically removed by the extension, which is not an option for *Hidden Costs* as those costs are permanently integrated in the process. In contrast, *Hidden Costs* had the codes "popup", "shortcut/skip steps" and "inform about manipulation", which aimed to inform the user about the hidden costs earlier, which counters the pattern well.

As expected, *Hidden Costs* and *Sneak Into Basket* shared a lot of similarities

The other combination of deceptive patterns where we suspected some similarities was *Dead End*, *Feedforward Ambiguity* and *Privacy Maze*. As seen in Figure 4.2, the bar charts for *Dead End* and *Privacy Maze* look very similar, while *Feedforward Ambiguity* has more "information", but less "automated". Two countermeasure ideas with slight variations were suggested and winning for all three of the patterns. The first idea was automatically offering, replacing or rerouting links. This makes sense as it offers an option out for *Dead End* and reduces confusion error rate for *Feedforward Ambiguity* and *Privacy Maze*. The second idea was automatically setting settings or denying or completing popups, which helps the user avoid the deceptive pattern altogether. For all three, participants were worried about the browser extension making mistakes and were critical towards automatically doing things because it could make mistakes or leave them stranded in the middle of an interaction. Especially for *Feedforward Ambiguity* and *Privacy Maze*, participants also placed importance on the customizability of the countermeasure, which makes sense as

Dead End and *Privacy Maze* were very similar, while there were some differences for *Feedforward Ambiguity*

for *Dead End*, there are not a lot of possibilities to personalize the suggested countermeasures. There was a lot of overlap between the most common codes, with all three having "autofill/-run", "shortcut/skip steps", "popup", and "link other pages". All of these seem sensible for these patterns. Interestingly, "solves similar problem" occurred multiple times. This was due to participants circumventing the need to access the privacy settings entirely by setting them automatically to the user's previously decided preferences. While this does not help the user find the privacy settings if they want to change something, this eliminates a lot of the need to and saves the user time, assuming they can trust the reliability of the countermeasure. There were of course also differences between the patterns, for example *Dead End* and *Feedforward Ambiguity* hat some ideas with "highlight" and "inform about manipulation", while *Privacy Maze* did not. In the designs for *Dead End* and *Privacy Maze*, there were some ideas using AI, while there were none for *Feedforward Ambiguity*. This is interesting because one might expect that to weaken *Feedforward Ambiguity*, one could use a system that considers how a user would understand the options and compare this to what the options actually do. This could have potential to warn the user about discrepancies, which was not one of the options the participants suggested.

4.1.3 Most Common Codes

The most common codes were for information, automation and visual changes

Overall, the most common codes (codes that were used 25 or more times) were: "popup" (27), "inform about manipulation" (27), "autofill/-run" (38), "shortcut/skip steps" (39), "spatial change" (34), "visually display/modify" (34), "reduction" (36) and "additional information" (36). From this, we can conclude that users want information and automation, and that users often think visual or spatial changes can counter deceptive patterns. Similarly, Lu et al. [2024] found three main strategies for deceptive pattern intervention employed by users, where these most common codes fit in as well. Their participants' main strategies were interface design change (which matches the codes "spatial change" and "visually dis-

play/modify"), user flow adjustment ("popup", "autofill/-run" and "shortcut/skip steps") and behavioral outcome reflection ("inform about manipulation" and "additional information"). The only one of our most used codes that is not reflected in their strategies is "reduction", which we used to describe countermeasures that reduce the deceptive pattern's effect but may not counter it completely.

The most commonly used top level code was "visual"

The most commonly used top level code was "visual" with 102 usages. Next were "information" with 82 usages, automated with 59, "intrusive" with 54. Lastly, "removing/reducing" was used 48 times. This highlights a big focus on visual changes and information, but also frequent usage of other ways to deal with deceptive patterns.

Some codes were only used for specific patterns

What might also be interesting to look at are the codes that were used only a few (<10) times or for specific patterns. For "entertainment" (5), "link other pages" (3) and "search feature" (2) it makes sense that they were only used a few times, as they usually describe individual features that are pretty pattern specific, and "add feature" (9) also summarized some very specific features such as adding an undo option or resetting all selected checkboxes. The only exception to that might be "entertainment", which could be included in more countermeasures, as the participants that discussed it for *Forced Work* seemed happy with the idea of having a "likable extension, one that makes you happy when you see it" (P15).
There are also some codes that were used less than 10 times that surprised us, as we would have expected them to be applied more. The first one was "assistant" (5), which seems like it could offer help against many different deceptive patterns. However, it was only suggested for the patterns *Temporal* and *Infinite Scrolling*. Especially *Temporal* obviously profits from an assistant that simplifies the entire process and all the deceptive patterns, and *Infinite Scrolling* is obvious as well, as an assistant that reminds you about your scrolling time might have more appeal than a simple message between the posts. However, for patterns like *Feedforward Ambiguity*, *Choice Overload* or *Privacy Maze*, we could have imagined an assistant being a suggested countermeasure, as it would help navigate through the confusion, similar to the ones suggested for the *Temporal* pattern.

The second code that was used less than expected was "AI" (4). Since artificial intelligence was a popular and controversial topic in the discussions, we would have expected to see more ideas utilizing it. For this, we need to consider that oftentimes participants did not explicitly state how the countermeasure should detect or evaluate something, which could often be done using AI.
Lastly, many participants consider personalizability an important aspect of countermeasures, naming the use cases of differing preferences, user groups or websites. Still, "customizable/disableable" (9) was not explicitly mentioned in a lot of designs. In some discussions, it was mentioned as an option after the design phase was over. There was no strong concentration of the code on specific patterns. Mostly, customizability was mentioned generally as an aspect that most or all countermeasures and the choice of countermeasure should have.

4.1.4 Code Combinations

There were some frequent code combinations. All of them fit together well

Some code combinations occurred more frequently than others. The most prominent one was "autofill/-run + shortcut/skip steps". These two fit together well, as to skip steps that are necessary for an interaction, one needs to automate them in some way.
"popup" was often combined with "friction" and "inform about manipulation". These fit well, too, as popups are a very simple way of implementing friction and conveying warnings.
There were also the combinations of "remove feature" with "autofill/-run" and "reduction". Especially the latter makes sense, as having less features often removes some options that could be manipulative or simply reduces the overload the user faces, as for example for the pattern *Choice Overload*. The first combination also makes sense in a way, as it can remove features that may be necessary by automatically dealing with them and then removing them. An example for this would be a countermeasure suggested for *Bad Defaults*, which automatically dealt with the confirmation window we used as an example by denying all "bad" options. This however takes the option of doing the

settings autonomously from the user.
"autofill/-run + customizable/disableable" was also a popular combination. It makes sense that users want the ability to personalize something that is done automatically so they can be sure it does exactly what they want.
The last combination was "spatial change + reduction". Through spatial changes, participants often achieved a weakening of the manipulation. This was especially evident in the countermeasures for *Nagging*, which were mostly ideas that changed the location of the presented information and weakened the pattern by making it less intrusive and repeated.

4.1.5 Bright Patterns

The code "reverse manipulation" was given a total of 15 times. The patterns where it was used in countermeasures were *Confirmshaming*, *Bad Defaults*, *Feedforward Ambiguity*, *Infinite Scrolling* and *Forced Work*.

Bright patterns occurred in the form of emotional manipulation, shaming, obstruction, visual prominence and anti-personalization

First, we will consider in which way "reverse manipulation" was used in the countermeasure designs.
There were four instances of *Emotional Manipulation*, with three of them being *Negative Framing* and one being *Cuteness*. *Shaming* was used three times between the patterns *Confirmshaming* and *Infinite Scrolling*, either to reverse the deceptive pattern's shaming or to stop the user from scrolling, both of which seem effective. Used five times was *Obstruction*, mostly for *Bad Defaults* and also for *Infinite Scrolling*. For *Bad Defaults*, the participants described their ideas as automatically deselecting all options and then hiding or completely removing the "bad" options to stop the user from selecting them. This is also what Graßl et al. [2021] found to be effective. They found that setting defaults is very powerful, and obstruction the user from "bad" options helps them change their behavior. For *Infinite Scrolling*, the ideas were to make it harder for the user to keep scrolling by blocking posts or reducing the quality of the site. Findings by Meinhardt et al. [2025] suggest that in some contexts, more extreme interventions are nec-

essary to stop the user from scrolling, which is in line with our findings. Used twice was *Visual Prominence*, where the options the extension deemed as "good" were highlighted in green and the "bad" ones in red for each. Lastly, *Anti-Personalization* was used once to replace personalized content with the opposite or boring content to reduce the user's interest.

Participants concluded that manipulating the user for their own benefit was justifiable

Participants discussed the topic of manipulating the user for good every time it was suggested. One participant said that while it was also manipulative, they thought of it as a compromise because the user was being manipulated in both directions at the same time. Another participant contemplated if manipulation in itself was unethical, as it takes away the user's autonomy. However, they also arrived at the conclusion that only manipulation against one's own interests was unethical. This assumes that the user's intentions are always clear, which can not always be assumed. We argue that in most cases, deceptive patterns act against the user's interests, therefore bright patterns probably manipulate in the user's best interest.
When discussing their countermeasures for *Infinite Scrolling*, participants remarked that this was a pattern where it is easy to manipulate the user, because the countermeasure actually wants to manipulate the user to stop scrolling. One participant also said that they did not like the shaming countermeasures as it made them feel bad.

4.1.6 Solving Similar Problems

There were some ideas that did not solve the deceptive pattern directly

For some countermeasures, we gave the code "solves similar problem" to indicate designs that were primarily aimed at solving a different problem than the presented deceptive pattern. These ideas circumvent the pattern instead of countering it directly. One could argue that these ideas did not fulfill the task, as they did not exactly counter the deceptive pattern they were supposed to counter. However, one could also argue that working around it is a better solution than nothing. Most of these ideas still have positive effects on the user experience. It is also interesting to see

what approaches participants had, even if they were not perfectly matched to the problem.

For example, for *Privacy Maze* and *Dead End*, there were ideas that reduced the need for the user to search for their settings by adjusting them automatically or restricting data sharing. These ideas would make it less likely that the user needs to find something but do not help them if they do.

For *Feedforward Ambiguity*, there was the same suggestion twice, which was to automatically choose one of the options the user could be confused by. This has the problem that it requires the extension to know where the user wants to go. Furthermore, it does not help the user understand the options any better and therefore also avoids the problem rather than solve it. Another idea for *Feedforward Ambiguity* was to rephrase the informational text. Again, this does not help the user understand where their options lead but rather strengthen the desire to choose the right one, which does not solve the problem. If done correctly, however, it could lead the user to understand the options better.

For *Forced Registration*, there was one suggestion to remove the "hook" of the website and move the registration prompt to the very beginning. While this may weaken the user's motivation to comply with the registration, it does not remove the problem of there being a mandatory registration to access the content locked behind it.

Lastly, this code was given for a solution for the second variant of the *Temporal* pattern. One participant suggested displaying how many other websites also sell the article the user is interested in. While this counters some deceptive patterns like *Urgency* and offers alternatives the user can visit if they are for example unhappy with the amount of deceptive patterns on one site, it does not remove most of the manipulation from the original site. This means it does not help the user for example if they have to buy from this specific site for whatever reason.

Most ideas that did not perfectly solve the deceptive pattern reduced the need for the user to interact with it or strengthened their motivation to resist it.

4.2 User Preferences

4.2.1 Questionnaire

Participants wanted less responsibilities placed on the user and suggested laws multiple times

Even though laws were not the focus of this study, a few participants argued that they are the only real way to solve this. They wanted standardization of all legally binding fields and to always find all important information in the same place. Participants argued that you have to start with the website's developers. This is reflecting Hinds et al. [2020], who discussed whether the responsibility of dealing with deceptive patterns should lie with the user or with organizations. Drawing from their comments, our participants came to the conclusion that they do not think users should be responsible for this. They also wanted to display the legal framework in case of violations. By doing this, some participants made it clear that they do not think technical countermeasures are an adequate solution for deceptive patterns. While working laws would be the ideal solution, as we discussed in Section 2.2 "Countermeasures", the approach of outlawing deceptive patterns faces many difficulties and is currently not realistic on its own.

Some participants' preferences contradict each other

There were some answers by different participants that contradicted each other, indicating points where user preferences vary strongly, which should be considered when implementing countermeasures. Some participants wanted to see exactly what countermeasures were applied to which deceptive patterns, while others did not want to be confronted with the issue at all. This is also shown by the fact that users both wished for noticeable countermeasures to preserve transparency, but also for subtle ones to not impact the user experience too much. To aim for transparency but also to not bother the user is challenging to realize at the same time, as the countermeasure has to provide all the requested information somehow, but can also not be too aggressive with it as this would annoy the user.
There was also a contradiction between participants who wanted a simple set-and-forget solution and participants who wanted a lot of customizability for choosing counter-

measures for each website individually. Both of these perspectives make sense, as users can have different standards for different websites, for example based on trust [Bhoot and Shinde, 2020] or the need to use a specific website, but also be overwhelmed if countermeasures are too complicated. The participants said that if setting up a countermeasure took too long, they would rather accept the manipulation than deal with the process, which is in line with the finding by Jung et al. [2022] that convenience outweighs privacy concerns. Combining these is another challenge for countermeasure design, as customizing something is a burden to the user.

4.2.2 Reoccurring Discussion Topics

There were reoccurring topics in both the design rounds and the final discussions, with partially contrary opinions between groups.

Popups were controversial

A controversial topic were popups. While many participants included them in their countermeasures somewhere, most agreed that they could become annoying and ineffective quickly, and should be used with caution. As literature [Jung et al., 2022; Inal et al., 2024] confirms that popups and similar elements, such as cookie consent banners, are rarely read by participants, this is definitely a point that should be considered. When most users would just ignore a countermeasure because they are used to ignoring annoying popups, the countermeasure barely has any effect. For some patterns, like *Infinite Scrolling*, they might be one of the best solutions, so designers have to consider that users automatically rarely read popups, even when they know they should. One option to utilize them well is, as a participant mentioned in their final questionnaires, giving the user the option to end something like a subscription immediately.

Participants were concerned about countermeasures making errors

In terms of mistake tolerance, participants were concerned whether the countermeasures would work reliably. As Schäfer et al. [2023] found, trust in a countermeasure is very important. One participant also said that it was im-

portant to them that countermeasures were deterministic, which suggests that LLMs are not the perfect solution for all implementations. Additionally, one participant wanted the countermeasures to notice on its own when it can not handle a deceptive pattern and react appropriately. This is of course a valid wish, as it would make it easier to trust a countermeasure's reliability. However, this is also hard to achieve on a technical level and may therefore not be entirely realistic. For example, during deceptive pattern detection, if a countermeasure does not detect a deceptive pattern, how would it notice? And if it did detect a deceptive pattern where there is none, it would treat it like one and not notice either.

Simplicity was universally important to participants

All participants shared the same opinion that simplicity was important. While Habib et al. [2022] investigated cookie acceptance behavior and not countermeasures, they also found that users will go for the easiest option. One participant also commented on a specific countermeasure, saying that they would be most likely to use this one because it does not require any input from them. Lastly, in agreeance with the finding by King and Stephan [2021] that simply giving more checkboxes or options does not solve the problem, one participant said that the example for the *Temporal* pattern was too complex, which is why they would only remove things and not add anything in fear of making it more chaotic.

As a general countermeasure, participants suggested a report system

While multiple participants suggested some kind of report system as a general countermeasure and to be effective against future patterns, one participant added moderation by experts as a requirement for it to work. Another participant ruled it out completely, saying that it would be too prone to abuse by bad actors. These are valid concerns, so while something similar might help recognize future patterns and warn users, it would have to be heavily moderated to make sure no dangerous content is recommended to users, which in turn would increase administrative effort and costs by a lot and prevent it from being automated completely, unless Artificial Intelligence reaches a stage where it can reliably replace experts in scenarios like this.

Warning, highlighting and educating were popular countermeasure ideas as well. One participant said that spreading digital literacy and general distrust in the internet would be the only thing that could really help. However, many participants recognized that they know they are unable to resist advertisements, personalization, or sales and countdown timers. This is in line with Susser et al. [2019] arguing that problematizing personalization is one step to weaken online manipulation. One participant took their inability to resist as a reason to argue that for them, the best countermeasure would be completely removing these things and not confronting them with it at all. Bongard-Blanchy et al. [2021] found that users can not consistently resist deceptive patterns even when they recognized them, supporting these concerns. On the other hand, Ye et al. [2025] found that experiential learning can help users cope with deceptive patterns, which suggests that simply telling the user about deceptive patterns is not an effective countermeasure, but training coping mechanisms could be a viable way to help users deal with them on their own.

Participants suggested educating users to resist deceptive patterns but acknowledged that it would not help for many patterns

4.2.3 Other Discussion Topics

One participant brought up the topic of paying for websites and also for countermeasures. They took the position that they were fine with paying for things that they use on a daily basis, as long as they're not being tricked or drained of money. They were fine with paying "a small editorial office's rent, but not for corporate greed" (P15) because they would "rather pay with my money than with my time" (P15). They also mentioned that they would consider both an open source or paid countermeasure okay, as long as it was a one-time payment and not a subscription. To our knowledge, the topic of paying for countermeasures has not been discussed yet. They would have to be non-profit to reduce the risk of manipulating the user. However, having a higher budget might increase the possibilities, for example administrative burdens like monitoring user suggestions could be covered by this.

Other interesting discussion topics include paying for countermeasures and supporting the user in doing something instead of doing something for them

One participant also raised the interesting point that all of their ideas were something the computer could do for the user and not "what could the user do themselves where an extension could support them" (P15). Supporting the user instead of just doing something for them is an interesting perspective on countermeasures. Many of the suggested countermeasures that were informing, made visual changes or added features and content could fall into the category of being support rather than doing everything. On the other hand, there were a lot of suggestions for "automated" and "altered user experience", which were less supportive and more on the side of doing something for the user. For some patterns, doing something might be more effective, like *Infinite Scrolling* where participants remarked that "to be effective for me, it has to be completely blocked" (P6), which is not supporting the user but rather doing something for them. On the other hand, as Jarovsky [2018] argues that countermeasures should not be paternalistic but rather support the user in decision-making, many patterns offer opportunities for countermeasures that do exactly that. Examples for countermeasure ideas that support the user in doing something could be informing about the manipulation or consequences, which were used for many patterns such as *Sneak Into Basket*, *Hidden Costs* or *Feedforward Ambiguity*. On the contrary, ideas that did something for the user were skipping an entire interaction automatically, which was used for multiple patterns, including *Forced Work*, *Temporal*, *Bad Defaults* and *Feedforward Ambiguity*.

Participants discussed being used to deceptive patterns and trusting some companies more than others

Other points that were discussed were already being used to the presence of deceptive patterns and recognizing that this lowered their standards for a trustworthy website, which is in line with findings by Di Geronimo et al. [2020]. One participant even commented that while on some websites like Temu[1] , the amount of deceptive patterns made them leave the site, while on Amazon[2] they barely noticed them, even though another participant commented that Amazon utilizes a lot of them. This is in line with the finding by Bhoot and Shinde [2020] that users are more willing to accept deceptive patterns when they already trust a

[1] `https://www.temu.com`, *last accessed September 28, 2025*
[2] `https://www.amazon.com/`, *last accessed September 28, 2025*

company. It also supports findings by Gray et al. [2020] that users will sometimes stop using websites that manipulate them. One user claimed something that went in a similar direction, saying they have already looked for solutions to some of the patterns and therefore were less creative when coming up with new ones.

Participants were worried about countermeasures being distracting

In one group there was a discussion about countermeasures being distracting, which they said would be very bad for them as they already want to do too many things at once, so a countermeasure should not add to that. One participant said that this would be fine for them, but another argued that this would be "dangerous" (P15) for their ADHD. Mildner et al. [2025] found something similar, with their findings showing that ADHD individuals have less predictable responses to deceptive patterns and that their attention and impulsivity vary significantly. One participant discussed the effects of different modalities. When talking about a digital assistant on the screen, they raised the concern that while on a computer, this would work well, but on a smartphone, it would take up too much space on the screen. Similarly, Gunawan et al. [2021] also argued that there is a need to research the differences in deceptive patterns between websites and mobile apps. This could be extended to countermeasures, as there might be differences in platform affordances, capabilities, and design norms [Gunawan et al., 2021] that could also impact what and how countermeasures work best in each modality.

Some countermeasures would work better on big screens

4.2.4 Transferability

An interesting point we wanted to look at was which countermeasures could be transferred to other patterns than the one they were designed for, or to future deceptive patterns that do not have specific countermeasures yet.

During the final discussion, we asked participants which countermeasures they thought would be applicable to other patterns as well. A common answer was highlighting the manipulation and informing the user about it, or spreading general awareness to train the user, which is gen-

erally applicable to all patterns, even if it may not guarantee protection [Bongard-Blanchy et al., 2021].

Participants suggested highlighting, information, AI, a report system and legal regulations as transferable countermeasures

Another idea was to train an AI to recognize and counter deceptive patterns in general, which is also promising if it is trained very generalized and one can assume that the error rate declines in the future. We also observed that an AI clicking through the page and warning the user about upcoming deceptive patterns was suggested for multiple patterns, including *Temporal*, *Dead End* and *Sneak Into Basket*, for which it was also the winning countermeasure. We draw the conclusion that this idea is very transferrable to other patterns as well.

Suggested multiple times with slight variations was having a report system where users could flag deceptive patterns or new manipulative design, which would then be verified and result in a warning for other users. In theory, this idea should work well, as it focuses on patterns that frustrate users and has potential to generate a lot of user input. However, previous research has shown that users are not able to recognize even popular deceptive patterns [Di Geronimo et al., 2020; Keleher et al., 2022; Seaborn et al., 2024], so it is reasonable to assume that they would also not consistently recognize new manipulation.

An idea that is applicable to all patterns but not implemented quickly is legal regulations, which were also brought up. Finally, participants suggested working with color or outsourcing all information into a separate, neutral formatting to counter visual manipulation, which should work for most visual patterns.

Other transferable countermeasures could be automatically denying and blocking unnecessary interactions, automatically adjusting settings, friction design and allowing the user to skip steps

There were also some solutions that participants did not explicitly mention that we consider transferable or that were suggested in similar forms for multiple patterns.

One idea for *Feedforward Ambiguity* was to automatically deny or block not necessary popups. This could also be applied to other patterns such as *Confirmshaming*, *Nagging*, *Choice Overload* or *Bad Defaults*. There is even more potential to use this with patterns we did not include in our study, such as *Interface Interference* or *Attention Capture*.

For both *Privacy Maze* and *Dead End*, there was the idea of automatically adjusting settings according to the user's preference to reduce the need to look for the settings in the first place, and for *Choice Overload* there was the similar

idea to automatically choose an option based on the user's preferences. This could also be applied to *Bad Defaults*, *Confirmshaming*, *Nagging* and other patterns.
Friction design occurred in countermeasures for many patterns, most notably for *Confirmshaming*, *Infinite Scrolling*, *Bad Defaults* and *Feedforward Ambiguity*. Generally, it could be applicable to all patterns that work off of the user's confusion or by sneaking something past them.
Lastly, for *Temporal*, *Forced Work* and *Privacy Maze* there were multiple ideas that allowed the user to skip steps or the entire process. This should also be a good countermeasure for many deceptive patterns: If the user can choose the outcome and have the countermeasure complete the entire process, they are not confronted with any of the manipulation they might face otherwise.

4.3 Intervention Space

In this section, we want to investigate how the countermeasures that were suggested in our user study fit into the intervention space by Bongard-Blanchy et al. [2021], which is shown in Figure 2.1.

We place the suggested countermeasures by our participants in the intervention space by Bongard-Blanchy et al. [2021]

The technical measures "automated detection tools" and "plug-ins" or "add-on extensions" were generally assumed as a base assumption or software for all countermeasure ideas by our participants. This makes sense, as we asked them to focus on technical countermeasures and explained how automated detection could work and how countermeasures can intervene into a website.

Some things were mentioned for general countermeasures, such as the educational and regulatory measures. While participants were worried about actually resisting deceptive patterns, they mentioned general education as the most broadly applicable countermeasure. Legal regulations were mentioned as the easiest, most effective and, for some participants, ideal countermeasure.

All the aspects Bongard-Blanchy et al. [2021] mentioned in the design column also appeared in our results. "Warnings" were utilized when informing users about the manipulation, which was one of the most common codes. "Reframing costs" was used by rephrasing options and informational texts and also informing the user about consequences of actions to resist the manipulation. Especially for the pattern *Infinite Scrolling*, but also for confirmations for other patterns and more, participants used "Friction Design". "Bright Patterns", while being a controversial topic, were also used in designs a notable amount of times. Lastly, "transparency impact assessment" was mentioned tangentially by some participants saying they want to know how manipulative a website is and one participant suggesting a "mental health score" to assess how bad a website is for them. "Design Guidelines" were also mentioned in the form of some participants wishing for standardization and obligatory neutral wordings of all legally binding fields.

4.4 Research Question

RQ How do users want countermeasures to handle deceptive patterns?

Considering everything we discussed about our results, we have some answers to our research questions. Based on the most common codes in the countermeasure designs as well as the discussions, users want countermeasures to handle deceptive patterns reliably and either automatically but not silently, with visual changes or with additional information. They would prefer laws to technical countermeasures and want as little additional effort for the user as possible. We also found that customizability is a very important aspect, both within countermeasures as well as between user groups and websites, as user preferences and needs vary strongly.

4.5 Limitations

When discussing our results, we also have to consider the challenges our study faced. We mentioned some of the general study design limitations beforehand and below, we will discuss the main limitations of our work.

All of our participants had a technical background

The first limitation is in our participant demographic. While we had an even ratio of female and male participants and a fairly even distribution of previous deceptive pattern knowledge, all of our participants were university students in technical subjects, mostly computer science. They also all reported feeling capable of using the internet well (M = 4.5, SD: 0.49) and spending 3-5 or 5+ hours a day using the internet. This limits the generalizability of our findings, as we worked with a user group with a strong technical background and a lot of experience using the internet, which not all users have.
The age range of our participants was also very limited, with the youngest being 20 and the oldest 28. This of course leaves out a big demographic of internet users.

Some groups had fewer participants, which resulted in less data. We also have to consider the effects of participant's personal opinions and the bias introduced through our examples

During the study, some cancellations resulted in three groups having only two participants instead of three, as seen in Table 3.1. We also observed that some groups were less talkative or had more trouble coming up with designs than others, which resulted in having less data to work with from these groups. Therefore, there are less design ideas and opinions for some patterns, while others had groups of three participants and long discussions.
Due to the overall participant count being 18, there were only 2 to 3 participants that designed countermeasures for each pattern. This means that personal opinions and preferences had a strong effect on the countermeasure ideas, which we need to keep in mind when discussing our findings. The participants with a lot of previous knowledge could also have been influenced by existing literature and taken ideas from there.
While we were careful to not introduce any bias when talking about deceptive patterns and countermeasures in general, we have to consider that the examples we chose for our study introduced bias. For some patterns (*Feedforward*

Ambiguity, *Nagging*, *Forced Registration*), we noticed that some of the countermeasures were very tailored to the specific example we showed our participants and not the pattern in a broader sense. This still allows us to draw conclusions about user preferences and ideas for countermeasures, but limits the generalizability of our findings to all occurrences of these patterns.

Users are not professional designers

Generally, as we discussed in 3.2 "Method", there are some fundamental aspects of our study design that may limit the generalizability of our findings. To recap, we have to consider user designs carefully as users are not designers and may not know about good design principles, and that our study's participants knew the deceptive pattern as well as the countermeasure, while in real-world application, users would only see the countermeasure. This needs to be something we consider when we base future work on our findings.

Our taxonomy may need to be reworked with our findings in mind

Finally, we may need to reconsider some categories of our own deceptive pattern taxonomy. We believe that creating it to allow a countermeasure-oriented exchange was the right idea. However, our findings have shown that our categories might need to be reworked, as some patterns in the same categories had vastly different countermeasures. One example of patterns that could belong in the same category are *Dead End*, *Privacy Maze* and *Feedforward Ambiguity*, which had similar distributions of their top level codes and all operate by confusing the user. Still, we only tested 2-3 patterns per category, so the lack of overlap could be explained by that, which means we need further testing to decide on the validity of our categories.

Chapter 5

Summary and Future Work

In this section, we summarize our findings and provide an overview of our contributions. Finally, we draw some conclusions for future work that could build on this thesis.

5.1 Summary and Contributions

In this thesis, we aimed to understand how users want countermeasures to handle deceptive patterns. For this, we mainly focused on countermeasure ideas, where we collected visual designs. Secondly, we investigated general user preferences. We did this through a study with an elicitation style drawing part and focus group discussions. In total, we had 18 participants in 7 groups. They redesigned two deceptive patterns per group for a total of 14 patterns. We chose the deceptive patterns for our study from our own countermeasure-oriented taxonomy to have a variety of pattern types and a framework for our analysis. The study was structured into two design rounds with a short discussion and a final discussion and questionnaire afterward.

In total, we received 179 countermeasure drawings. The participants' ideas were mostly focused on visual countermeasures, followed by automated and informational ones. Some of the suggested countermeasure ideas were already suggested in literature and have been proven to be effective. There were also some popular designs that have not been researched yet but from our analysis have been shown to be viable ideas.
During the discussions, it became clear that users valued different things, meaning customizability is an important factor. Universally important were simplicity, transparency and autonomy, while some users also wanted automation and entertainment. On the other hand, participants did not want a complicated setup process, an annoying user experience or high error rates. Some more controversial topics were popups, hiding content and bright patterns.

In summary, this thesis contributes an approach for a countermeasure-oriented taxonomy, ideas for countermeasures and possibilities for how to handle new and future deceptive patterns. Finally, we also provide insights into what is important to users in countermeasures. Further research is needed to verify and test these user preferences, and to implement and test the most popular suggested countermeasures for their real-world usability. We discuss possible approaches for this in the following section.

5.2 Future Work

Future work could remedy our limitations

One direction for future work could be to conduct a similar study while fixing some of our study's limitations. It could be interesting to see what countermeasures other user groups, for example users with little technical background, would come up with and whether they would have different priorities. Insights into this might allow for more broadly usable countermeasures that can help a bigger audience.

Our countermeasure ideas could be implemented and tested

Another step future work could take is taking some of the most popular countermeasure ideas from our study and implement prototypes to test out their technical feasibil-

ity and user acceptance. Testing them in a dedicated user study may reveal which countermeasures actually work in a real usage scenario and reveal new priorities for countermeasures that did not come up in a theoretical space. Even if the exact designs are not technically feasible or work well in a realistic situation, the general ideas are worth considering.

Our findings on user preferences can be considered for future countermeasure design and research

Lastly, our findings from the discussion, such as customizability, simplicity, and transparency should be considered for future countermeasure design to ensure that countermeasures fulfill user preferences. Some of the more controversial topics could also be investigated further to examine why users have certain preferences and how they affect their liking of certain countermeasures.

Appendix A

Deceptive Pattern Definitions, Taxonomy and Examples

This appendix contains the definitions of all patterns investigated in our study. It also includes the categorization of patterns from Gray et al. [2024] and others into our own taxonomy as described in section 3.2.1 "Countermeasure-oriented Taxonomy" as well as pictures of the deceptive pattern examples used in our study.

A.1 Taxonomy

The patterns we selected for our study are written in *Italics*. Additionally we classify other low- and meso-level patterns from Gray et al. [2024] that are mentioned in this thesis.

Category	Patterns
Manipulated Information	*Hidden Costs* *Feedforward Ambiguity* Trick Question Language Inaccessibility Manipulating Choice Architecture False Hierarchy Visual Prominence
Obstruction	*Forced Work* *Dead End* *Privacy Maze* Roach Motel Creating Barriers
Cognitive Bias	*Infinite Scrolling* *Bad Defaults* *Choice Overload* Personalization Emotional or Sensory Manipulation
Pressuring	*Nagging* *Confirmshaming* Urgency Scarcity and Popularity Claims
Taking Away Agency	*Sneak Into Basket* *Forced Registration* Forced Communication or Disclosure
Temporal	*Variant 1* *Variant 2*

A.2 Definitions and Examples

Here, we will provide definitions of all deceptive patterns included in our study. Additionally, we include the examples we used to present them during the study. All of the visualizations have been created on our own custom website prototype and were fully interactive. Participants were presented with these website snippets on a monitor and showed an interaction with them. We will include translations of the text for each pattern (from left to right, top to bottom, with line breaks represented by "-").

Figure A.1: Example of *Hidden Costs* in an online shopping checkout context.

Hidden Costs: Gray et al. [2024] define Hidden Costs as delaying revealing the full price of a product of service through late or incomplete disclosure, which misleads the user about the full price when making a purchase decision.

Page 1: "Cart - 1x Pants 19,95€ - 1x T-Shirt 15,95€ - Sum: 35,90€ - Continue to payment".
Page 2: "Payment - Sum: 35,90€ - Back to Cart - Payment Details - Address - Name - Street - City - Choose Payment Method - Credit Card - Finish".
Page 3: "Summary - Your Order - 1x Pants 19,95€ - 1x T-Shirt 15,95€ - Back to Cart - Shipping: 3,99€ - Processing Fee: 4,99€ - Service Fee: 4,99€ - Total: 49,87€ - Order".

Figure A.2: Example of *Feedforward Ambiguity* in a notification consent popup, where the button labeled "Verwerfen" (Dismiss) accepts the notifications.

Feedforward Ambiguity: "Feedforward Ambiguity subverts the user's expectations that their choice will be likely to result in an action they can predict, instead providing a discrepancy between information and actions available to users that results in an outcome that is different from what the user expects" [Gray et al., 2024].

Page 1: "Do you want to receive notifications? - We will only send you important notifications. - Yes - Dismiss".
Page 2: "Thank you! - We will send you notifications from now on."

Figure A.3: Example of *Forced Work* where the user is forced to watch an advertisement before they can download a file.

Forced Work: Forced Work deliberately increases work for the user, for example by forcing them to wait and watch an advertisement [Conti and Sobiesk, 2010].

Page 1: "Start Download - You want to download this file: - example.pdf - Start download".
Page 2: "Please wait... - Before starting your download, please watch this advertisement. - Your advertisement could be here! - Advertisement running: 5 seconds remaining - Continue".
Page 3: "Download - Your download is starting now. - Go back".

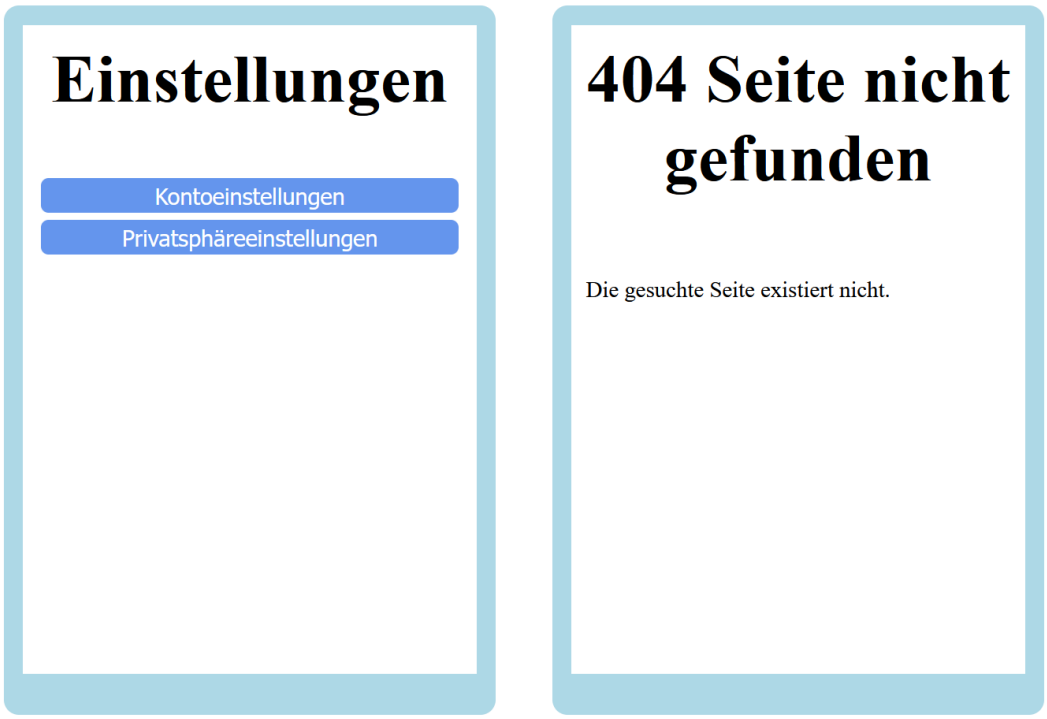

Figure A.4: Example of *Dead End* where the user is blocked from finding their privacy settings.

Dead End: Dead End prevents users from finding information or options through inactive links, leaving them unable to achieve their goal [Gray et al., 2024].

Page 1: "Settings - Account settings - Privacy settings".
Page 2: "404 Page not found - The page you are looking for does not exist."

Figure A.5: Example of *Privacy Maze* where the user is obstructed when trying to change their settings for personalized advertisements.

Privacy Maze: Privacy Maze forces the user to navigate through many pages to access information or options without providing a comprehensive overview to prevent them from easily discovering relevant information or action possibilities [Gray et al., 2024].

Page 1: “Manage Settings - Here you can manage your account settings. - Edit profile - Notifications - Friends - Security - Help”.
Page 2: “Privacy & Security - Manage your privacy settings. - Change password - 2-factor authentication - Manage data sharing - Go back”.
Page 3: “Manage Data Sharing - Your data is used to improve your experience - Learn more - Personalized advertisements - Data sharing - Go back”.
Page 4: “Personalized Advertisements - You see personalized advertisements based on your data. - Accept - Deny - Go back”.

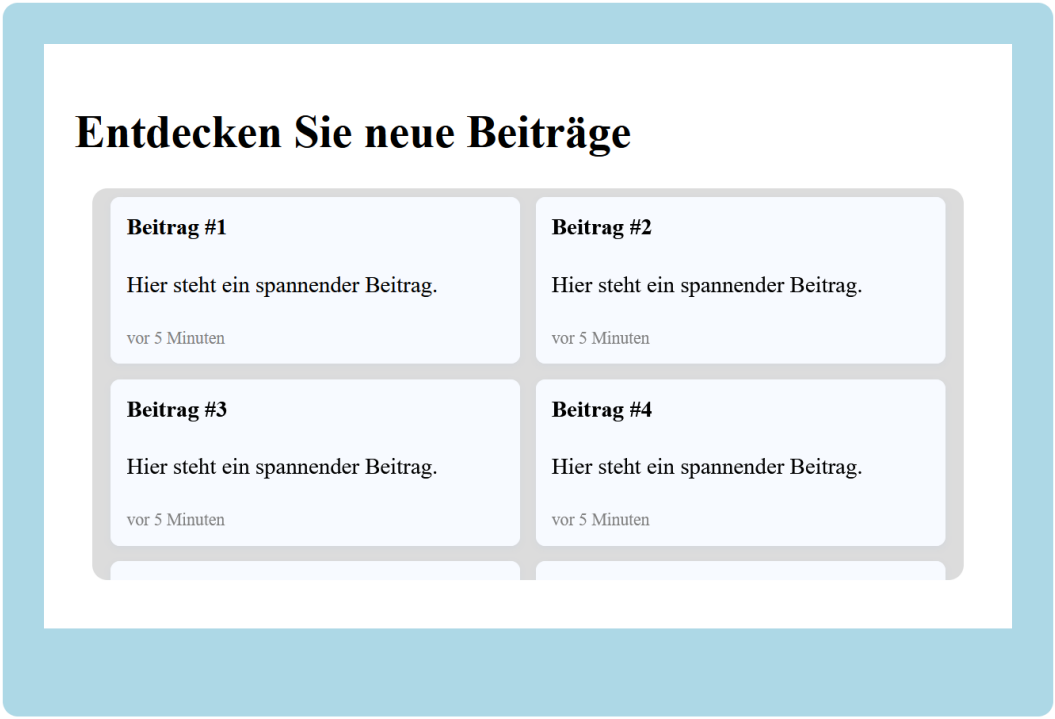

Figure A.6: Example of *Infinite Scrolling* where there are infinite posts on a page.

Infinite Scrolling:

Translation: “Discover new Posts - Post 1 - This is an interesting post - 5 minutes ago - ...”

Figure A.7: Example of *Bad Defaults* for newsletters and privacy settings.

Bad Defaults: Bad Defaults builds on the user's assumptions that the default settings will be in their best interest and requires them to take active steps to change settings that are not set in their favor by default [Gray et al., 2024].

Translation: "Welcome to our Website! - Thank you for your registration! We are happy to have you here. - Confirm your settings and start immediately. - Newsletter & Settings - I want to regularly receive advertising emails. - My data may be used for personalized advertising. - My data may be shared with third parties. - Only allow necessary cookies. - Confirm".

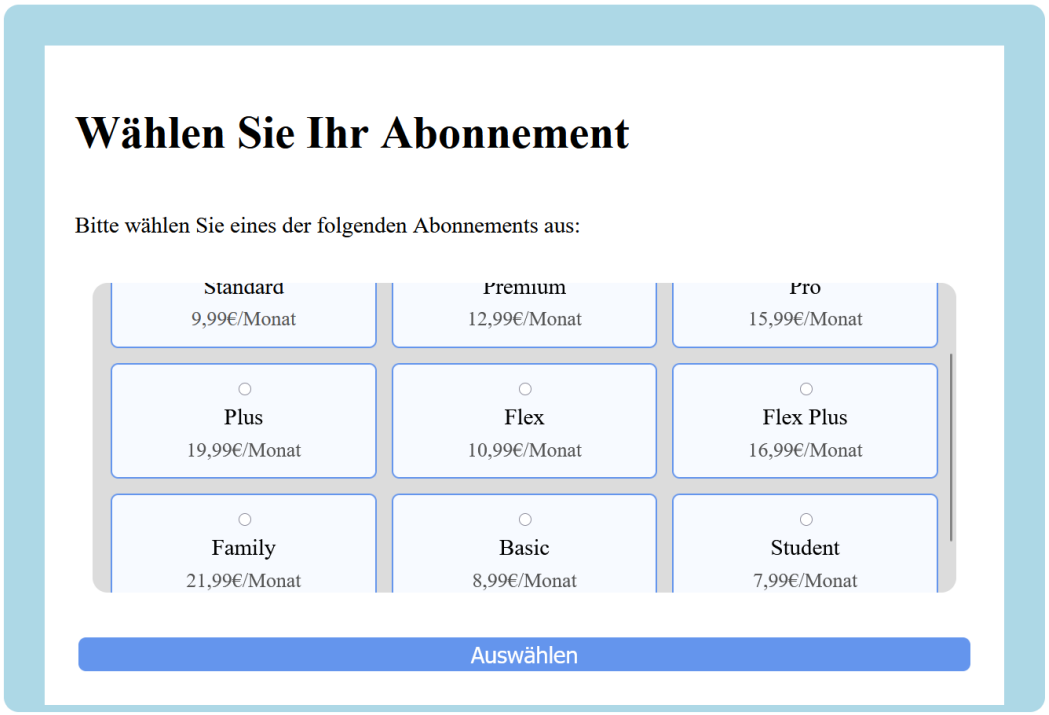

Figure A.8: Example of *Choice Overload* in the context of choosing a subscription.

Choice Overload: Choice Overload provides too many options to understand or compare, which leads the user to overlook relevant information and make uninformed decisions [Gray et al., 2024].

Translation: "Select your Subscription - Please select one of the following subscriptions: - Standard 9,99€/month - Premium 12,99€/month - Pro 15,99€/month - Plus 19,99€/month - Flex 10,99€/month - Flex Plus 16,99€/month - Family 21,99€/month - Basic 8,99€/month - Student 7,99€/month - Select".

Figure A.9: Example of *Nagging*, repeatedly asking the user to register for a newsletter.

Nagging: Nagging repeatedly interrupts the user during a normal interaction to distract them from their task to have them make a decision they don't want to make [Gray et al., 2024].

Background: "Download file - You want to download this file: - example.pdf - Download".
Foreground: "Subscribe to our Newsletter! - Don't miss any more deals. Subscribe now! - Subscribe now - No thanks".

Figure A.10: Example of *Confirmshaming* that shames the user into subscribing to a newsletter.

Confirmshaming: Gray et al. [2024] define Confirmshaming as using "Personalization as a type of Social Engineering to frame a choice to opt-in or opt-out of a decision through emotional language or imagery that relies upon shame or guilt. As a result, the user may be convinced to change their goal due to the emotionally manipulative tactics, resulting in being steered away from making a choice that matched their initial goal."

Translation: "Subscribe to Newsletter - Do you want to receive exclusive news and offers? - Email - Yes, I want to save! - No, I like paying more."

Figure A.11: Example of *Sneak Into Basket* where premium shipping is automatically added to the basket.

Sneak Into Basket: Sneak Into Basket adds unwanted items to a user's shopping cart without their knowledge, which leads to unintentional purchase of additional items [Gray et al., 2024].

Page 1: "Cart - 1x Pants 19,95€ - 1x T-Shirt 15,95€ - Sum: 35,90€ - Continue to payment".
Page 2: "Payment - Sum: 40,89€ - Premium shipping has been automatically added for you. - Back to cart - Payment details - Address - Name - Street - City - Choose payment method: - Credit card - Finish".
Page 3: "Cart - 1x Pants 19,95€ - 1x T-Shirt 15,95€ - 1x Premium shipping 4,99€ - Sum: 40,89€ - Continue to payment".

Figure A.12: Example of *Forced Registration* where the user is forced to register before continuing to read a newspaper article.

Forced Registration: Forced Registration forces users to register or create an account to complete an action that they thought was possible without doing so [Gray et al., 2024].

Translation: "Breaking News - On Saturday morning, there was a police operation in downtown Aachen. This happened: ... - Read the full article and many more with a free account: - Email - Password - Repeat password - Sign up & keep reading - Email - Password - Sign in".

Figure A.13: Example of a combination of patterns (*Temporal* Variant 1) in a subscription canceling interaction.

Temporal Variant 1: The definition of temporality by Gray et al. [2025] is the interplay of deceptive patterns across a user journey. We adapted the first variant from Gray et al. [2025], where they depict an Amazon[1] subscription canceling process.

[1] `https://www.amazon.com/`, *last accessed 28.09.2025*

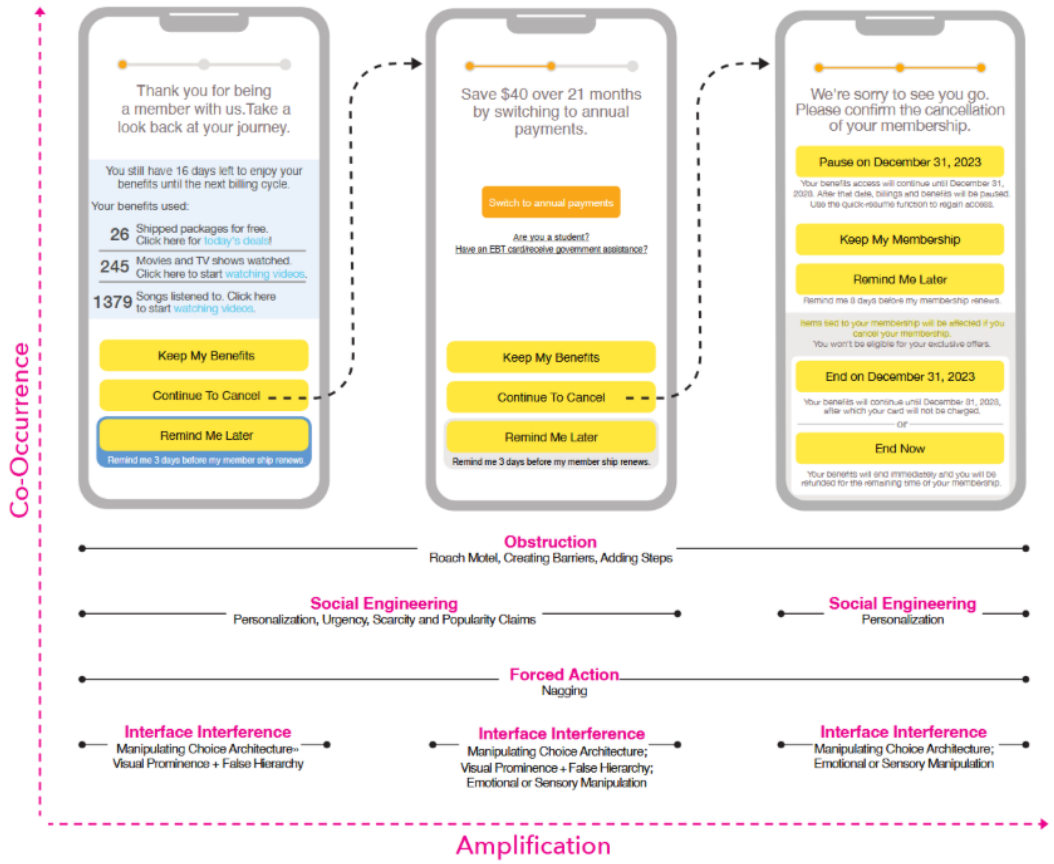

Figure A.14: The original *Temporal* image from Gray et al. [2025], which we translated to German for our study (see Figure A.13). All included patterns are listed in the image.

Temporal Variant 2: This variant of the Temporal category was created by us, simulates a fictional online shopping checkout process and contains the patterns *Sneak Into Basket*, *Urgency*, *Personalization*, *Emotional or Sensory Manipulation*, *Confirmshaming*, *Forced Registration*, *False Hierarchy*, *Hidden Costs* and *Bad Defaults*.

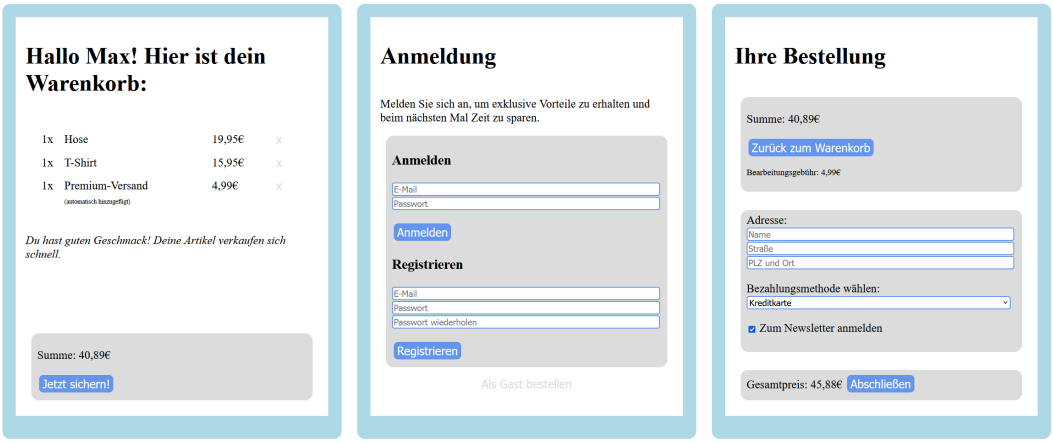

Figure A.15: Example of a combination of patterns (*Temporal* Variant 2) in an online shopping checkout process.

Page 1: "Hello Max! Here is your cart: - 1x Pants 19,95€ - 1x T-Shirt 15,95€ - 1x Premium shipping 4,99€ - (added automatically) - You have good taste! Your articles are selling fast. - Sum: 40,89€ - Secure now!".
Page 2: "Registration - Sign up now to receive exclusive benefits and save time next time. - Sign in - Email - Password - Sign up - Email - Password - Repeat password - Sign up - Order as guest".
Page 3: "Your order - Sum: 40,89€ - Back to cart - Processing fee: 4,99€ - Address: - Name - Street - City - Choose payment method: - Credit card - Subscribe to newsletter - Total: 45,88€ - Finish".

Appendix B

Questionnaires

The questionnaires used for the demographic data collection as well as the countermeasure design templates and the final questionnaire are attached in the following. The English translation of the German questionnaires is provided in section B.2 “Questionnaires (English)”.

B.1 Questionnaires (German)

Einwilligung zur Studienteilnahme

Studie: Eliciting Countermeasures Against Deceptive Patterns

Studienleitung: Julia Kemp
RWTH Aachen
julia.kemp@rwth-aachen.de

Zweck der Studie: Das Ziel dieser Studie sind Einblicke in die Vorstellungen von Nutzenden für Maßnahmen gegen Deceptive Patterns. Hierzu werden die Teilnehmenden zu den präsentierten Deceptive Patterns Gegenmaßnahmen designen.

Ablauf: Nachdem demographische Daten gesammelt wurden, wird den Teilnehmenden ein Deceptive Pattern präsentiert und der manipulative Aspekt erklärt. Daraufhin werden sie Gegenmaßnahmen malen und Anmerkungen zu diesen machen. Anschließend gibt es eine Diskussion über die entstandenen Gegenmaßnahmen und die Teilnehmenden markieren danach ihre Favoriten. Dies wird für insgesamt zwei Deceptive Patterns durchgeführt. Abschließend wird es eine Diskussionsrunde über Gegenmaßnahmen im Allgemeinen und einen abschließenden Fragebogen zur Verschriftlichung der allgemeinen Ideen geben. Die Studie wird etwa zwei Stunden dauern. Während der Studie wird eine Audioaufzeichnung gemacht, die der Auswertung der Diskussionen dient.

Risiken: Die Studie hält keine körperlichen oder psychischen Risiken bereit. Die Teilnehmenden werden manipulatives Design sehen, aber über dieses aufgeklärt und nicht hinters Licht geführt werden. Sollte eine Aufgabe oder Diskussion einem Teilnehmenden nahegehen, wird diese unverzüglich abgebrochen.

Vorteile: Die Ergebnisse dieser Studie werden benutzt, um besser zu verstehen, mit welchen Gegenmaßnahmen Nutzende vor Deceptive Patterns geschützt werden wollen.

Alternativen zur Teilnahme: Die Teilnahme an der Studie ist freiwillig und kann jederzeit ohne Konsequenzen abgebrochen werden.

Kosten und Aufwandsentschädigung: Bei der Studie werden keine Kosten für die Teilnehmenden entstehen. Es werden Snacks und Getränke bereitgestellt. Nach der Studie wird unter den Teilnehmenden, unabhängig vom Inhalt der Studie, eine Amazon-Gutschein im Wert von 20€ verlost.

Vertraulichkeit: Alle in der Studie gesammelten Daten werden vertraulich behandelt. Alle Daten werden durch Teilnehmendennummern anonymisiert. Keine aus dieser Studie entstehenden Arbeiten oder Publikationen werden Informationen enthalten, die Rückschlüsse auf die Person der Teilnehmenden erlauben.

Wenn du an der Studie teilnehmen möchtest, unterschreibe bitte unten.

◯ Ich habe die Informationen gelesen und verstanden.
◯ Die Informationen wurden mir erklärt.

_____	_____	_____
Name	Datum, Ort	Unterschrift

_____
E-Mail-Adresse (optional, für die Teilnahme am Gewinnspiel)

_____	_____
Datum, Ort	Unterschrift Studienleitung

Julia Kemp (Kontakt: julia.kemp@rwth-aachen.de) P___

Bachelorarbeitsstudie zu Countermeasures für Deceptive Patterns

Demographische Daten

Alter: _____

Geschlecht: _____

Aktuelle Tätigkeit:

◯ *Studium*: Studiengang: _____, angestrebter Abschluss: _____

◯ *Arbeit*: _____

◯ *Ausbildung*: _____

◯ *Sonstiges*: _____

Technische Kenntnisse:

Internetnutzung täglich in Stunden:

◯ <1 ◯ 1-3 ◯ 3-5 ◯ >5

„Ich verbringe viel Zeit auf Online-Shopping-Seiten."

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

„Ich fühle mich fähig im Umgang mit dem Internet."

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

„Mir ist Sicherheit im Internet wichtig."

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

„Ich achte bei meinem Verhalten im Internet auf Sicherheit."

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

„Ich habe nie Probleme damit, auf Internetseiten mit den gegebenen Funktionen das zu erreichen, was ich vorhabe (z.B. Einstellungen ändern oder Produkte kaufen)."

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

Dark/Deceptive Pattern Vorwissen:

„Ich wusste vor dieser Studie bereits, was Dark/Deceptive Patterns sind."

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

Definiere „Dark/Deceptive Pattern": _____

_____

_____

_____

weiter auf der Rückseite

Definition Deceptive Pattern:

Deceptive Patterns (ursprünglich Dark Patterns) sind Elemente von Benutzeroberflächen, die so gestaltet sind, dass sie die Entscheidungen des Nutzenden manipulieren und seine Autonomie beeinträchtigen.

Beispiele für Kategorien von Deceptive Patterns:

- *Sneaking*: Patterns, die wichtige Informationen verstecken oder verzögern, sodass der Nutzende eine Handlung durchführt, die nicht in seinem Interesse ist und der er andernfalls nicht zugestimmt hätte
- *Obstruction*: Patterns, die eine Interaktion unterbrechen oder erschweren und den Nutzenden dadurch von einer Handlung abhalten
- *Interface Interference*: Patterns, die die Benutzeroberfläche manipulieren, um bestimmte Handlungsmöglichkeiten über andere zu stellen
- *Forced Action*: Patterns, in denen der Nutzende dazu gezwungen wird, bewusst oder unbewusst eine zusätzliche Handlung durchzuführen, um seine Interaktion mit dem System fortsetzen zu können
- *Social Engineering*: Patterns, die erwartete oder erzeugte soziale Normen benutzen, um den Nutzenden durch die dargestellten Möglichkeiten oder Informationen zu einer bestimmten Handlung zu drängen

In dieser Studie verwenden wir den Begriff Deceptive Patterns.

„Ich begegne im Internet häufig Deceptive Patterns.“

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

„Ich bin anfällig Deceptive Patterns gegenüber.“

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

„Ich denke, dass Menschen in meinem Umfeld im Internet häufig Deceptive Patterns begegnen.“

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

„Ich denke, dass Menschen in meinem Umfeld anfällig Deceptive Patterns gegenüber sind.“

Stimme überhaupt nicht zu ◯ ◯ ◯ ◯ ◯ Stimme voll zu

Julia Kemp (Kontakt: julia.kemp@rwth-aachen.de) P___

Bachelorarbeitsstudie zu Countermeasures für Deceptive Patterns

Pattern: _____

1	2
Anmerkungen:	Anmerkungen:
3	4
Anmerkungen:	Anmerkungen:

Julia Kemp (Kontakt: julia.kemp@rwth-aachen.de) P___

Bachelorarbeitsstudie zu Countermeasures für Deceptive Patterns

Abschließende Fragen:

Was ist dir bei Countermeasures im Allgemeinen wichtig?

Hast du bei deinen favorisierten Countermeasures Gemeinsamkeiten bemerkt?

Wie würde deine ideale Countermeasure aussehen?

Wie könnte man Countermeasures designen, um in Zukunft mit neuen Deceptive Patterns umzugehen, bevor es für diese spezifische Countermeasures gibt?

Weitere Anmerkungen:

B.2 Questionnaires (English)

Informed Consent

Study: Eliciting Countermeasures Against Deceptive Patterns

Principal Investigator: Julia Kemp
RWTH Aachen
julia.kemp@rwth-aachen.de

Purpose of the Study: The aim of this study is to gain insights into users' ideas for measures against deceptive patterns. To this end, participants will design countermeasures for the deceptive patterns presented.

Procedure: After demographic data has been collected, participants will be presented with a deceptive pattern and the manipulative aspect will be explained. They will then draw countermeasures and make comments on them. This will be followed by a discussion of the countermeasures that have been designed, after which participants will mark their favorites. This will be done for a total of two deceptive patterns. Finally, there will be a discussion round on countermeasures in general and a concluding questionnaire to write down the general ideas. The study will take about two hours. An audio recording will be made during the study to evaluate the discussions.

Risks: The study does not pose any physical or psychological risks. Participants will see manipulative design, but will be informed about it and will not be deceived. If a task or discussion upsets a participant, it will be stopped immediately.

Benefits: The results of this study will be used to better understand what countermeasures users want to protect themselves from deceptive patterns.

Alternatives to Participation: Participation in the study is voluntary and can be discontinued at any time without consequences.

Cost and Compensation: There will be no costs for participants in the study. Snacks and drinks will be provided. After the study, an Amazon voucher worth €20 will be raffled off among the participants, regardless of the content of the study.

Confidentiality: All data collected in the study will be treated confidentially. All data will be anonymized using participant numbers. No work or publications resulting from this study will contain information that allows conclusions to be drawn about the identity of the participants.

If you agree to participate in this study, please sign below.

◯ I have read and understood the information on this form.
◯ I have had the information on this form explained to me.

_____	_____	_____
Name	Date, City	Signature

_____
Email address (optional, for participation in the raffle)

_____	_____
Date, City	Principal Investigator’s Signature

Julia Kemp (Email: julia.kemp@rwth-aachen.de) P___

Bachelor's Thesis Study on Countermeasures Against Deceptive Patterns

Demographic Data

Age: _____

Gender: _____

Occupation:

◯ *Studying*: Course: _____, degree: _____

◯ *Work*: _____

◯ *Apprenticeship*: _____

◯ *Other*: _____

Technical knowledge:

Daily Internet usage in hours:

◯ <1 ◯ 1-3 ◯ 3-5 ◯ >5

„I spend a lot of time on online shopping websites."

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

„I feel capable of using the Internet."

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

„I value Internet security."

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

„I pay attention to security when using the Internet."

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

„I never have any problems using the functions provided on websites to do what I want to do (e.g., change settings or buy products)."

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

Dark/Deceptive Pattern knowledge:

„I knew what Dark/Deceptive Patterns are before participating in this study."

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

Define „Dark/Deceptive Pattern": _____

_____

_____

_____

continue on the next page

Definition Deceptive Pattern:

Deceptive patterns (originally dark patterns) are elements of user interfaces that are designed to manipulate the user's decisions and impair their autonomy.

Examples of categories of deceptive patterns:

- *Sneaking*: Patterns that hide or delay important information so that the user performs an action that is not in their interest and to which they would not otherwise have agreed
- *Obstruction*: Patterns that interrupt or hinder interaction, thereby preventing the user from performing an action
- *Interface Interference*: Patterns that manipulate the user interface to prioritize certain actions over others
- *Forced Action*: Patterns in which the user is forced to consciously or unconsciously perform an additional action in order to continue interacting with the system
- *Social Engineering*: Patterns that use expected or created social norms to push the user toward a specific action through the options or information presented

In this study, we use the term “deceptive patterns.”

„I run into a lot of deceptive patterns when using the Internet.“

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

„I am vulnerable to deceptive patterns.“

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

„I think that people around me run into a lot of deceptive patterns when using the Internet.“

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

„I think that people around me are vulnerable to deceptive patterns.“

Completely disagree ◯ ◯ ◯ ◯ ◯ Completely agree

Julia Kemp (Email: julia.kemp@rwth-aachen.de) P___

Bachelor's Thesis Study on Countermeasures Against Deceptive Patterns

Pattern: _____

1	2
Comments:	Comments:
3	4
Comments:	Comments:

Julia Kemp (Email: julia.kemp@rwth-aachen.de) P___

Bachelor's Thesis Study on Countermeasures Against Deceptive Patterns

Final Questions:

What is important to you in countermeasures in general?

Have you noticed any similarities between your favorite countermeasures?

What would your ideal countermeasure look like?

How could countermeasures be designed to deal with new deceptive patterns in the future before specific countermeasures exist for them?

Additional comments:

Appendix C

Codebook

The following codebook contains all codes derived from thematic analysis in Chapter 3 “User Study”. It is important to note that the frequency of higher level codes is based on the number of distinct segments matching the code, not just the sum of the subcodes. A graph displaying the frequencies of the "Countermeasure Ideas" codes can be found in Fig. 3.6.

Code	Frequency
Countermeasure Ideas	
information	82
assistant	5
recommended action	10
rephrase	15
inform about manipulation	27
inform about consequences	20
search feature	2
link other pages	3
additional information (for the page itself)	36
automated	59
autofill/-run	38
shortcut/skip steps	39
visual	102
highlight	17
overlay	24
strike out/cover manipulation	18
spatial change	34
visually display/modify	34
intrusive	54
popup	27
reverse manipulation	15
friction	17
entertainment	5
add feature	7
removing/reducing	48
reduction	36
solves similar problem	10
remove feature	17
AI	4
customizable/disableable	9
Star ratings	**63**
>3 stars	1
3 stars	8
2 stars	21
1 star	33
2 stars by one person	9

Table C.1: Codebook containing all codes and categories for the countermeasure designs from the qualitative analysis from Chapter 4, and the respective number of distinct encoded segments

Code	Frequency
Final Questionnaire	**292**
technical feasibility/reliability	23
laws/standardization	17
user groups	9
report system	12
other aspects	33
visual	12
customizability	18
user experience	41
simplicity	48
information	40
transparency/autonomy	39

Table C.2: Codebook containing all codes and categories concerning the general discussions and questionnaire from the qualitative analysis from Chapter 4, and the respective number of distinct encoded segments

Bibliography

[1] Juris Hannah Adorna, Aurel Jared Dantis, Rommel Feria, Ligaya Leah Figueroa, and Rowena Solamo. Developing a Browser Extension for the Automated Detection of Deceptive Patterns in Cookie Banners. In *Proceedings of the Workshop on Computation: Theory and Practice (WCTP 2023)*, pages 101–120. Atlantis Press, 2024. doi.org/10.2991/978-94-6463-388-7_8.

[2] Ghada Alsebayel, Giovanni Maria Troiano, and Casper Harteveld. "Not Nice!": Towards Understanding Dark Patterns in Commercial Health Apps. In Colin M. Gray, Johanna Gunawan, René Schäfer, Nataliia Bielova, Lorena Sánchez Chamorro, Katie Seaborn, Thomas Mildner, and Hauke Sandhaus, editors, *Proceedings of the Workshop Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024)*, volume 3720 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2024.

[3] Carlos Bermejo Fernandez, Dimitris Chatzopoulos, Dimitrios Papadopoulos, and Pan Hui. This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), October 2021. doi.org/10.1145/3476087.

[4] Aditi Bhoot and Mayuri Shinde. Towards the Identification of Dark Patterns: An Analysis Based on End-User Reactions. In *11th Indian Conference on Human-Computer Interaction*, pages 24–33, 11 2020. doi.org/10.1145/3429290.3429293.

[5] John B. Black and Thomas P. Moran. Learning and remembering command names. In *Proceedings of the 1982 Conference on Human Factors in Computing Systems*, CHI '82, page 8–11, New York, NY, USA, 1982. Association for Computing Machinery. doi.org/10.1145/800049.801745.

[6] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele 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*,

DIS '21, page 763–776, New York, NY, USA, 2021. Association for Computing Machinery. doi.org/10.1145/3461778.3462086.

[7] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006. doi.org/10.1191/1478088706qp063oa.

[8] Harry Brignull. *Deceptive Patterns*. Testimonium Ltd, 2023. ISBN 978-1739454401.

[9] P. Burnard, P. Gill, K. Stewart, E. Treasure, and B. Chadwick. Analysing and presenting qualitative data. *British Dental Journal*, 204:429–432, 2008. doi.org/10.1038/sj.bdj.2008.292.

[10] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies*, page 237–254, 2016. doi.org/10.1515/popets-2016-0038.

[11] Jieshan Chen, Jiamou Sun, Sidong Feng, Zhenchang Xing, Qinghua Lu, Xiwei Xu, and Chunyang Chen. Unveiling the Tricks: Automated Detection of Dark Patterns in Mobile Applications. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*, UIST '23, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3586183.3606783.

[12] Gregory Conti and Edward Sobiesk. Malicious interface design: exploiting the user. In *Proceedings of the 19th International Conference on World Wide Web*, WWW '10, page 271–280, New York, NY, USA, 2010. Association for Computing Machinery. doi.org/10.1145/1772690.1772719.

[13] Andrea Curley, Dympna O'Sullivan, Damian Gordon, Brendan Tierney, and Ioannis Stavrakakis. The Design of a Framework for the Detection of Web-Based Dark Patterns. *ICDS 2021: The 15th International Conference on Digital Society*, 2021.

[14] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto 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*, CHI '20, page 1–14, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3313831.3376600.

[15] Directorate-General for Justice and Consumers (European Commission), F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, and T. Rodríguez de las Heras Ballell. *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation –*

Final report. Publications Office of the European Union, 2022. doi.org/10.2838/469916.

[16] Kevin Fiedler, René Schäfer, Jan Borchers, and René Röpke. "Deception Detected!"—A Serious Game About Detecting Dark Patterns. In Avo Schönbohm, Francesco Bellotti, Antonio Bucchiarone, Francesca de Rosa, Manuel Ninaus, Alf Wang, Vanissa Wanick, and Pierpaolo Dondio, editors, *Games and Learning Alliance*, pages 191–200, Cham, 2025. Springer Nature Switzerland. doi.org/10.1007/978-3-031-78269-5_18.

[17] Daniel Fitton, Janet C Read, Gavin Sim, and Brendan Cassidy. Co-designing voice user interfaces with teenagers in the context of smart homes. In *Proceedings of the 17th ACM Conference on Interaction Design and Children*, IDC '18, page 55–66, New York, NY, USA, 2018. Association for Computing Machinery. doi.org/10.1145/3202185.3202744.

[18] B. J. Fogg. Persuasive technology: using computers to change what we think and do. *Ubiquity*, 2002(December), December 2002. doi.org/10.1145/764008.763957.

[19] B. J. Fogg. A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology*, Persuasive '09, New York, NY, USA, 2009. Association for Computing Machinery. doi.org/10.1145/1541948.1541999.

[20] P. Gill, K. Stewart, E. Treasure, and B. Chadwick. Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, 204: 291–295, 2008. doi.org/10.1038/bdj.2008.192.

[21] Michael D. Good, John A. Whiteside, Dennis R. Wixon, and Sandra J. Jones. Building a user-derived interface. *Commun. ACM*, 27(10):1032–1043, October 1984. doi.org/10.1145/358274.358284.

[22] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–14, New York, NY, USA, 2018. Association for Computing Machinery. doi.org/10.1145/3173574.3174108.

[23] Colin M. Gray, Shruthi Sai Chivukula, and Ahreum Lee. What Kind of Work Do "Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, DIS '20, page 61–73, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3357236.3395486.

[24] Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, and Thomas Mildner. An Ontology of Dark Patterns Knowledge: Foundations, Definitions,

and a Pathway for Shared Knowledge-Building. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery. doi.org/10.1145/3613904.3642436.

[25] Colin M. Gray, Thomas Mildner, and Ritika Gairola. Getting Trapped in Amazon's "Iliad Flow": A Foundation for the Temporal Analysis of Dark Patterns. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery. doi.org/10.1145/3706598.3713828.

[26] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research*, 3(1):1–38, Feb. 2021. doi.org/10.33621/jdsr.v3i1.54.

[27] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), October 2021. doi.org/10.1145/3479521.

[28] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. "Okay, whatever": An Evaluation of Cookie Consent Interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery. doi.org/10.1145/3491102.3501985.

[29] Pelle Guldborg Hansen and Andreas Maaløe Jespersen. Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy. *European Journal of Risk Regulation*, 4(1):3–28, 2013. doi.org/10.1017/S1867299X00002762.

[30] S. M. Hasan Mansur, Sabiha Salma, Damilola Awofisayo, and Kevin Moran. AidUI: Toward Automated Recognition of Dark Patterns in User Interfaces. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, pages 1958–1970, 2023. doi.org/10.1109/ICSE48619.2023.00166.

[31] Philip Hausner and Michael Gertz. Dark Patterns in the Interaction with Cookie Banners, 2021. URL https://arxiv.org/abs/2103.14956.

[32] Joanne Hinds, Emma J. Williams, and Adam N. Joinson. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143:102498, 2020. doi.org/10.1016/j.ijhcs.2020.102498.

[33] Yavuz Inal, Frode S. Volden, Camilla Carlsen, and Sarah Hjelmtveit. My Eyes Don't Consent! Exploring Visual Attention in Cookie Consent Interfaces. In

Proceedings of the 2024 Symposium on Eye Tracking Research and Applications, ETRA '24, New York, NY, USA, 2024. Association for Computing Machinery. doi.org/10.1145/3649902.3653352.

[34] Luiza Jarovsky. Improving Consent in Information Privacy Through Autonomy-Preserving Protective Measures (APPMs). *European Data Protection Law Review*, 4:447–458, 2018. doi.org/10.21552/edpl/2018/4/7.

[35] Frederike Jung, Kai von Holdt, Ronja Krüger, Jochen Meyer, and Wilko Heuten. I do. Do I? – Understanding User Perspectives on the Privacy Paradox. In *Proceedings of the 25th International Academic Mindtrek Conference*, Academic Mindtrek '22, page 268–277, New York, NY, USA, 2022. Association for Computing Machinery. doi.org/10.1145/3569219.3569358.

[36] Maxwell Keleher, Fiona Westin, Preethi Nagabandi, and Sonia Chiasson. How Well Do Experts Understand End-Users' Perceptions of Manipulative Patterns? In *Nordic Human-Computer Interaction Conference*, NordiCHI '22, New York, NY, USA, 2022. Association for Computing Machinery. doi.org/10.1145/3546155.3546656.

[37] Dominique Kelly and Jacquelyn Burkell. Disclosure by Design: How Dark Patterns Reduce Users' Social Privacy. In Colin M. Gray, Johanna Gunawan, René Schäfer, Nataliia Bielova, Lorena Sánchez Chamorro, Katie Seaborn, Thomas Mildner, and Hauke Sandhaus, editors, *Proceedings of the Workshop Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024)*, volume 3720 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2024.

[38] Janice R. Kelly and Steven J. Karau. Entrainment of Creativity in Small Groups. *Small Group Research*, 24(2):179–198, 1993. doi.org/10.1177/1046496493242002.

[39] Rishabh Khandelwal, Thomas Linden, Hamza Harkous, and Kassem Fawaz. PriSEC: A Privacy Settings Enforcement Controller. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 465–482. USENIX Association, August 2021.

[40] Rishabh Khandelwal, Asmit Nayak, Hamza Harkous, and Kassem Fawaz. Automated cookie notice analysis and enforcement. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.

[41] Jennifer King and Adriana Stephan. Regulating privacy dark patterns in practice - drawing inspiration from california privacy rights act. *Georgetown Law Technology Review*, 2021.

[42] Kirill Kronhardt and Jens Gerken. Start Playing Around - Serious & Persuasive Games as a Viable Counter-Measure Against Deceptive Patterns? In Colin M. Gray, Johanna Gunawan, René Schäfer, Nataliia Bielova, Lorena Sánchez Chamorro, Katie Seaborn, Thomas Mildner, and Hauke Sandhaus, editors, *Proceedings of the Workshop Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024)*, volume 3720 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2024.

[43] Lin Kyi, Abraham Mhaidli, Cristiana Santos, Franziska Roesner, and Asia Biega. "It doesn't tell me anything about how my data is used": User Perceptions of Data Collection Purposes. In *CHI 2024 - Proceedings of the 2024 CHI Conference on Human Factors in Computing Sytems*, Conference on Human Factors in Computing Systems - Proceedings, United States, May 2024. Association for Computing Machinery. doi.org/10.1145/3613904.3642260.

[44] Frank Lewis and Julita Vassileva. Seeing in the Dark: Revealing the Relationships, Goals, and Harms of Dark Patterns. In Colin M. Gray, Johanna Gunawan, René Schäfer, Nataliia Bielova, Lorena Sánchez Chamorro, Katie Seaborn, Thomas Mildner, and Hauke Sandhaus, editors, *Proceedings of the Workshop Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024)*, volume 3720 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2024.

[45] Lassi A. Liikkanen, Tua A. Björklund, Matti M. Hämäläinen, and Mikko P. Koskinen. Time Constraints in Design Idea Generation. In *Proceedings of ICED 09, the 17th International Conference on Engineering Design*, ICED, Palo Alto, CA, USA, August 2009.

[46] Yuwen Lu, Chao Zhang, Yuewen Yang, Yaxing Yao, and Toby Jia-Jun Li. From Awareness to Action: Exploring End-User Empowerment Interventions for Dark Patterns in UX. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW1), April 2024. doi.org/10.1145/3637336.

[47] Jamie Luguri and Lior Jacob Strahilevitz. Shining a Light on Dark Patterns. *Journal of Legal Analysis*, 13(1):43–109, 03 2021. doi.org/10.1093/jla/laaa006.

[48] Maximilian Maier and Rikard Harr. Dark Design Patterns: An End-User Perspective. *Human Technology*, 16:170–199, 08 2020. doi.org/10.17011/ht/urn.202008245641.

[49] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019. doi.org/10.1145/3359183.

[50] Arunesh Mathur, Mihir Kshirsagar, and Jonathan 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*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery. doi.org/10.1145/3411764.3445610.

[51] Luca-Maxim Meinhardt, Maryam Elhaidary, Mark Colley, Michael Rietzler, Jan Ole Rixen, Aditya Kumar Purohit, and Enrico Rukzio. Scrolling in the Deep: Analysing Contextual Influences on Intervention Effectiveness during Infinite Scrolling on Social Media. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery. doi.org/10.1145/3706598.3713187.

[52] Thomas Mildner and Gian-Luca Savino. Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI EA '21, New York, NY, USA, 2021. Association for Computing Machinery. doi.org/10.1145/3411763.3451659.

[53] Thomas Mildner, Merle Freye, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. Defending Against the Dark Arts: Recognising Dark Patterns in Social Media. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, DIS '23, page 2362–2374, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3563657.3595964.

[54] Thomas Mildner, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3544548.3580695.

[55] Thomas Mildner, Daniel Fidel, Evropi Stefanidi, Paweł W. Woźniak, Rainer Malaka, and Jasmin Niess. A Comparative Study of How People With and Without ADHD Recognise and Avoid Dark Patterns on Social Media. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery. doi.org/10.1145/3706598.3713776.

[56] Stuart Mills and Richard Whittle. Detecting Dark Patterns Using Generative AI: Some Preliminary Results. *SSRN*, 2023. doi.org/10.2139/ssrn.4614907.

[57] Meredith Ringel Morris, Andreea Danielescu, Steven Drucker, Danyel Fisher, Bongshin Lee, M. C. Schraefel, and Jacob O. Wobbrock. Reducing legacy bias in gesture elicitation studies. *Interactions*, 21(3):40–45, May 2014. doi.org/10.1145/2591689.

[58] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana 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*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3313831.3376321.

[59] Deger Ozkaramanli, Elif Özcan, and Pieter Desmet. Long-Term Goals or Immediate Desires? Introducing a Toolset for Designing with Self-Control Dilemmas. *The Design Journal*, 20(2):219–238, 2017. doi.org/10.1080/14606925.2017.1272831.

[60] Lorenzo Porcelli, Michele Mastroianni, Massimo Ficco, and Francesco Palmieri. A User-Centered Privacy Policy Management System for Automatic Consent on Cookie Banners. *Computers 13*, 2024. doi.org/10.3390/computers13020043.

[61] Marie Potel-Saville and Mathilde Da Rocha. From Dark Patterns to Fair Patterns? Usable Taxonomy to Contribute Solving the Issue with Countermeasures. In *Privacy Technologies and Policy: 11th Annual Privacy Forum, APF 2023, Lyon, France, June 1–2, 2023, Proceedings*, page 145–165, Berlin, Heidelberg, 2023. Springer-Verlag. doi.org/10.1007/978-3-031-61089-9_7.

[62] Paul Preuschoff, Sarah Sahabi, René Schäfer, Lea Schirp, Marcel Lahaye, and Jan Borchers. Groups vs. Booking Websites: Investigating Collaborative Strategies Against Deceptive Patterns. In *Extended Abstracts of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI EA '25. Association for Computing Machinery, April 2025. doi.org/10.1145/3706599.3720225.

[63] S. Hrushikesava Raju, Saiyed Faiayaz Waris, S. Adinarayna, Vijaya Chandra Jadala, and G. Subba Rao. Smart Dark Pattern Detection: Making Aware of Misleading Patterns Through the Intended App. In Subarna Shakya, Valentina Emilia Balas, Sinchai Kamolphiwong, and Ke-Lin Du, editors, *Sentimental Analysis and Deep Learning*, pages 933–947, Singapore, 2022. Springer Singapore. doi.org/10.1007/978-981-16-5157-1_72.

[64] Karen Renaud, Cigdem Sengul, Kovila Coopamootoo, Bryan Clift, Jacqui Taylor, Mark Springett, and Ben Morrison. "We're Not That Gullible!" Revealing Dark Pattern Mental Models of 11-12-Year-Old Scottish Children. *ACM Trans. Comput.-Hum. Interact.*, 31(3), August 2024. doi.org/10.1145/3660342.

[65] Mathias Schlolaut, Olga Kieselmann, and Arno Wacke. Comparing Nudges and Deceptive Patterns at a Technical Level. In Colin M. Gray, Johanna Gunawan, René Schäfer, Nataliia Bielova, Lorena Sánchez Chamorro, Katie Seaborn, Thomas Mildner, and Hauke Sandhaus, editors, *Proceedings of the*

Workshop Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024), volume 3720 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2024.

[66] René Schäfer, Paul Miles Preuschoff, and Jan Borchers. Investigating Visual Countermeasures Against Dark Patterns in User Interfaces. In *Proceedings of Mensch Und Computer 2023*, MuC '23, page 161–172, New York, NY, USA, 2023. Association for Computing Machinery. doi.org/10.1145/3603555.3603563.

[67] René Schäfer, Paul Miles Preuschoff, René Röpke, Sarah Sahabi, and Jan Borchers. Fighting Malicious Designs: Towards Visual Countermeasures Against Dark Patterns. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery. doi.org/10.1145/3613904.3642661.

[68] René Schäfer, Sarah Sahabi, Lucia Karl, Sophie Hahn, and Jan Borchers. "If They Have No Choice, They'll Accept!": How Children and Adolescents Assess Deceptive Designs. In *Proceedings of the 24rd Annual ACM Interaction Design and Children Conference*, IDC '25, page 863–871. Association for Computing Machinery, June 2025. doi.org/10.1145/3713043.3731497.

[69] Katie Seaborn, Tatsuya Itagaki, Mizuki Watanabe, Yijia Wang, Ping Geng, Takao Fujii, Yuto Mandai, Miu Kojima, and Suzuka Yoshida. Deceptive, Disruptive, No Big Deal: Japanese People React to Simulated Dark Commercial Patterns. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '24, New York, NY, USA, 2024. Association for Computing Machinery. doi.org/10.1145/3613905.3651099.

[70] Ashutosh Singh, Nisarg Upadhyaya, Arka Seth, Xuehui Hu, Nishanth Sastry, and Mainack Mondal. What Cookie Consent Notices Do Users Prefer: A Study In The Wild. In *2022 European Symposium on Usable Security*, pages 28–39, 09 2022. doi.org/10.1145/3549015.3555675.

[71] Than Htut Soe, Cristiana Teixeira Santos, and Marija Slavkovik. Automated detection of dark patterns in cookie banners: how to do it poorly and why it is hard to do it any other way, 2022. URL https://arxiv.org/abs/2204.11836.

[72] D. A. Strauss. *Freedom of Speech*, chapter 3 - Persuasion, Autonomy, and Freedom of Expression. Routledge, 2000. doi.org/10.4324/9781315181981-3.

[73] Daniel Susser, Beate Roessler, and Helen F. Nissenbaum. Technology, Autonomy, and Manipulation. *Internet Policy Review*, 2019. doi.org/10.14763/2019.2.1410.

[74] Van Hong Tran, Aarushi Mehrotra, Ranya Sharma, Marshini Chetty, Nick Feamster, Jens Frankenreiter, and Lior Strahilevitz. Dark Patterns in the

Opt-Out Process and Compliance with the California Consumer Privacy Act (CCPA). In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery. doi.org/10.1145/3706598.3714138.

[75] Santiago Villarreal-Narvaez, Jean Vanderdonckt, Radu-Daniel Vatavu, and Jacob O. Wobbrock. A Systematic Review of Gesture Elicitation Studies: What Can We Learn from 216 Studies? In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, DIS '20, page 855–872, New York, NY, USA, 2020. Association for Computing Machinery. doi.org/10.1145/3357236.3395511.

[76] Jingzhou Ye, Yao Li, Wenting Zou, and Xueqiang Wang. From Awareness to Action: The Effects of Experiential Learning on Educating Users about Dark Patterns. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery. doi.org/10.1145/3706598.3713493.

Index

Typeset September 30, 2025