

Dissertation

**“DARK PATTERNS ON PRIVACY-RELATED WEB USER
INTERFACES”**

Eleni Loizou

UNIVERSITY OF CYPRUS



DEPARTMENT OF COMPUTER SCIENCE

May 2026

UNIVERSITY OF CYPRUS
DEPARTMENT OF COMPUTER SCIENCE

**DARK PATTERNS ON PRIVACY-RELATED WEB USER
INTERFACES**

Eleni Loizou

Supervisors

Dr. George Papadopoulos

Co-supervisor

Evangelia Vanezi

The Individual Diploma Thesis was submitted towards partially meeting the requirements for obtaining the degree of Computer Science of the Department of Computer Science of the University of Cyprus

May 2026

Acknowledgements

This thesis would not have been possible without the invaluable guidance, support, and encouragement I received throughout this journey.

First, I would like to sincerely thank my Supervisor, Dr. Giorgos Papadopoulos, for his trust and for giving me the opportunity to explore this topic. I am also deeply grateful to my Co-Supervisor and Researcher, Evangelia Vanezi, for her continuous support, insightful advice, and excellent collaboration during the development of this work. Their mentorship has been instrumental in helping me achieve my goals.

Finally, I wish to express my heartfelt thanks to my family, friends, and colleagues for their support, encouragement, and care throughout this endeavor.

I declare that this dissertation and any accompanying software are my own original work, conducted in full compliance with the University of Cyprus Code of Conduct for Research (<https://www.ucy.ac.cy/legislation/kodikas-deontologias-kai-politikes/>), and with full accountability on my part for the accuracy, integrity, and validity of all content.”

Abstract

Dark patterns are deceptive user interface designs that manipulate users into making choices they did not intend, often leading to unnecessary or unintended disclosure of personal data. These patterns can undermine individual privacy and conflict with legal requirements such as the General Data Protection Regulation (GDPR), which mandates clear and specific personal data collection practices. While previous research has examined dark patterns from theoretical, behavioral, legal, or empirical perspectives, this work focuses specifically on privacy-related dark patterns in web user interfaces and the development of a technical solution to address it.

In this thesis, a comprehensive list of dark patterns is compiled based on existing literature, followed by a manual audit of personal data collection interfaces on 81 popular websites to analyze the presence and prevalence of these patterns, and to collect information about each pattern. A taxonomy of dark patterns is developed informed by the data collected during the manual audit, including information such as detailed description, UI-level indicators and code level indicators, presented in both human-readable and machine-readable (JSON) formats.

Additionally, a user survey was conducted to evaluate how well users can identify dark patterns without support, highlighting the need for practical detection tools. To address this, the Dark Pattern Detection Tool was designed and implemented, which takes a website URL and the JSON taxonomy as input, identifies dark patterns present on the page, and provides detailed explanations while visually highlighting them on a live preview. The tool is evaluated with usability tests and user experience studies, demonstrating positive results in helping users be more confident in detecting dark patterns and raising their awareness on the topic.

Table of Contents

Chapter 1	1
Introduction.....	1
1.1 General Idea	1
1.2 Motivation.....	1
1.3 About the Tool.....	2
1.4 Structure of the Thesis	3
1.5 Research Methodology	3
Chapter 2	6
Background and Related Work.....	6
2.1 Introduction.....	6
2.2 Background	7
2.2.1 Privacy and Personal data protection in web platforms	7
2.2.2 Regulatory and legal context (GDPR and related principles)	8
2.2.3 Dark Patterns	9
2.3 Related Work	11
2.3.1 Works on the collection and processing of personal data on web platforms.....	11
2.3.2 Works on Dark Patterns in Websites/Web forms.....	13
2.4 List of the 25 Dark Patterns as extracted and compiled by the literature	15
Chapter 3	19
Dark Patterns in privacy collections UIs – the current web landscape	19
3.1 Introduction.....	19
3.2 Data Collection	19
3.3 Results	24
3.3 Conclusion	34
Chapter 4	35
A Taxonomy of Dark Patterns in Web Privacy	35
4.1 Introduction.....	35
4.2 Structure and Description of the Taxonomy	36
4.3 Human-readable format.....	39
4.4 Machine-readable format.....	40
Chapter 5	44
Run the Study: “A user study on the effects of dark patterns in their consent decisions.”	44
5.1 Introduction.....	44

5.2 Data Collection	44
5.3 Results	47
5.3.1 Demographic Results	47
5.2.2 Background Information Results	49
5.2.3 Dark Patterns on the Web Results	51
5.4 Conclusion	68
Chapter 6	70
A tool to assist in detecting and mitigating Dark Patterns	70
6.1 Introduction.....	70
6.2 Requirements	71
6.2.1 Functional Requirements	71
6.2.2 Non Functional Requirements.....	72
6.3 Design.....	73
6.4 Development	74
6.5 Tool Functionalities and Workflow.....	75
Chapter 7	79
Survey called “Dark Patterns Tool Feedback Survey”	79
7.1 Introduction.....	79
7.2 Data Collection	79
7.3 Results	83
7.3.1 Background Information Results	83
7.3.2 User Experience Evaluation Results	86
7.3.3 Usability and Acceptance Results.....	88
7.4 Conclusion	91
Chapter 8	92
Conclusion	92
8.1 Final Remarks	92
8.2 Future Work.....	92
B i b l i o g r a p h y	93
Appendix A.....	1
Appendix B	16
Appendix C.....	32
Appendix D.....	41
Appendix E	52

Chapter 1

Introduction

1.1 General Idea	1
1.2 Motivation.....	1
1.3 About the Tool.....	2
1.4 Structure of the Thesis	3
1.5 Research Methodology	3

1.1 General Idea

The central aim of this thesis is to examine how dark patterns influence user behavior in privacy-related interfaces of modern web applications and to provide a practical tool for enhancing transparency. Dark patterns are manipulative design techniques embedded in registration forms, consent dialogs, cookie banners, and account settings that often lead users to unintentionally share more personal data than they intend. Despite legal frameworks such as GDPR, users frequently encounter opaque or overly complex privacy notices, leaving them ill-equipped to make informed decisions.

This work investigates methods to empower users by making these manipulative designs visible and understandable. Through automated detection, detailed reporting, and interactive previews, the thesis demonstrates where dark patterns appear, what information they convey, and how they affect user consent. The study bridges user experience, legal compliance, and technical implementation to ensure that users can better detect, interpret, and resist dark patterns while providing actionable insights for developers and researchers to improve privacy interfaces.

1.2 Motivation

In today's digital environment, users routinely provide personal information online without fully understanding how it will be used. Despite regulations such as the General Data Protection Regulation (GDPR), privacy notices are often long, complex, and difficult to interpret. Users may overlook critical details, and the prevalence of dark patterns in web interfaces subtle manipulations designed to influence behavior further

complicates informed consent. These issues can result in unintended data sharing and undermine user trust.

At the same time, developers require practical solutions that are easy to implement, lightweight, and compatible with existing workflows. There is a need for approaches that enhance transparency without disrupting the overall design or functionality of web applications.

This thesis is motivated by the need to support both end-users and developers. For users, it aims to provide clear, actionable insights into where and how dark patterns appear, helping them make more informed privacy decisions. For developers and researchers, it provides a structured taxonomy to detect, analyze, and visualize dark patterns, encouraging the design of more ethical and user-friendly interfaces. By addressing these dual needs, the work contributes to a safer and more transparent digital ecosystem where personal data collection is both understandable and accountable.

1.3 About the Tool

To address the challenges identified in this thesis, the Dark Pattern Detection Tool was developed. This tool allows users to input the URL of any web page they wish to examine. Upon receiving a URL, the tool automatically detects privacy-related dark patterns present on the page and generates detailed information about each identified pattern.

In addition to textual reporting, the tool visually highlights dark patterns directly in a live website preview. This interactive display enables users to see exactly where and how each manipulative design appears, providing a clear, practical understanding of the interface's behavior. Users can explore both the type of dark pattern and the relevant information associated with it, making the identification process intuitive and actionable.

The tool is fully client-side and operates entirely within the browser, requiring no installation or server-side processing. By combining automated detection, interactive highlighting, and comprehensive explanations, the Dark Pattern Detection Tool

empowers users, researchers, and developers to analyze, understand, and mitigate dark patterns effectively, improving transparency and ethical design in web applications.

To develop our tool, we followed a research methodology by studying the literature, conducting a manual audit on popular websites, creating a taxonomy of dark patterns, and running a user survey to validate the need. The developed tool is informed by all the above, while it integrates the JSON format of the taxonomy.

1.4 Structure of the Thesis

The thesis is structured as follows. It begins with Chapter 1, which introduces the general idea of the work, explains the motivation for conducting the study, and provides an overview of the tool developed. Chapter 2 presents the background and related work, including the regulatory context, data collection practices on the web, and a review of dark patterns. Chapter 3 analyzes the prevalence and impact of dark patterns in privacy collection interfaces on current websites. Chapter 4 presents a taxonomy of dark patterns, detailing both human-readable and machine-readable representations. Chapter 5 describes the design and results of a user study examining the effects of dark patterns on consent decisions. Chapter 6 discusses the design, development, and functionalities of the tool created to detect and mitigate dark patterns. Chapter 7 reports on the feedback survey conducted to evaluate the tool's usability, user experience, and acceptance. Finally, Chapter 8 concludes the thesis with final remarks and outlines directions for future work. The bibliography lists all references used throughout the study.

1.5 Research Methodology

The study combines literature review, taxonomy design, manual website analysis, and practical software development in order to investigate the use of dark patterns in modern web applications. The methodology was designed to support both the theoretical understanding of manipulative interface techniques and the practical implementation of a detection tool capable of identifying such patterns in websites.

The research methodology followed a structured, five-phase workflow, as illustrated in the following diagram.

1. Phase 1 – Data Collection:

Conducted a literature review to compile a comprehensive list of dark patterns.

Performed a manual audit of 81 websites to determine the prevalence and distribution of these patterns and gather all needed information.

2. Phase 2 – Modelling:

Developed a taxonomy of dark patterns, represented in human-readable format for comprehension and as JSON for automated detection.

3. Phase 3 – User Survey:

Evaluated users' ability to recognize and understand dark patterns, highlighting gaps in awareness that the tool needs to address.

4. Phase 4 – Tool Development:

Built a web-based tool capable of detecting dark patterns and providing identification and explanations.

5. Phase 5 – Tool Evaluation:

Assessed the tool's effectiveness in helping users detect and understand dark patterns, informing iterative improvements.

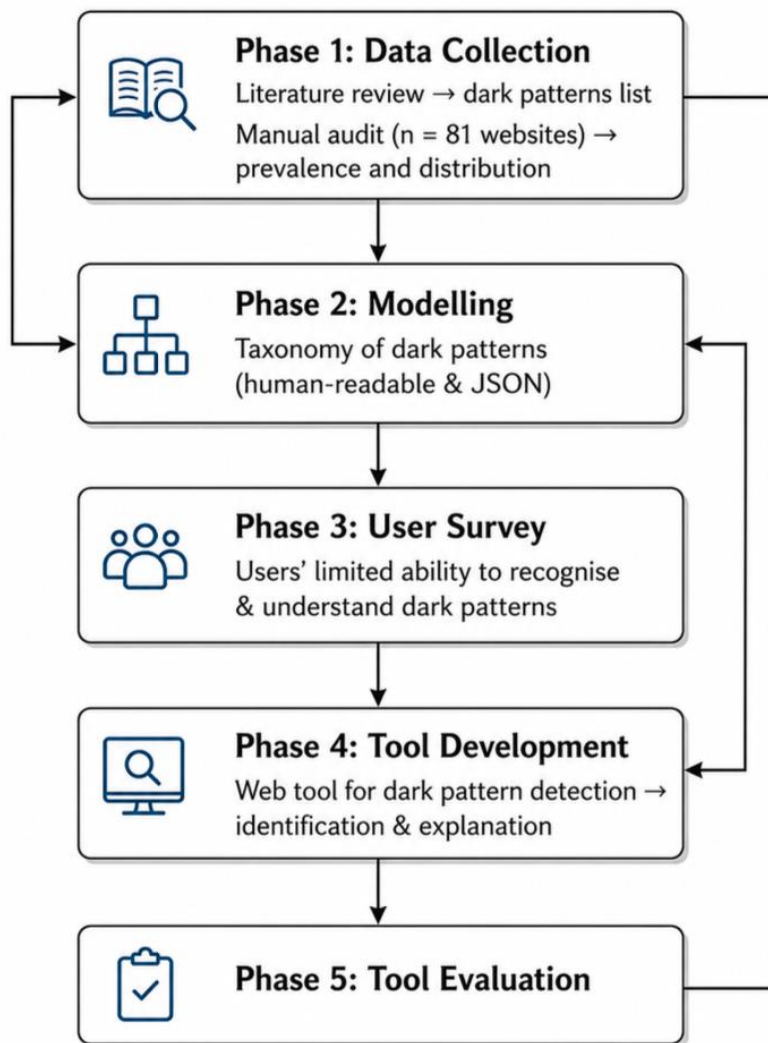


Figure 1.1: Research Methodology Diagram

Chapter 2

Background and Related Work

2.1 Introduction.....	6
2.2 Background	7
2.2.1 Privacy and Personal data protection in web platforms	7
2.2.2 Regulatory and legal context (GDPR and related principles)	8
2.2.3 Dark Patterns	9
2.3 Related Work	11
2.3.1 Works on the collection and processing of personal data on web platforms.....	11
2.3.2 Works on Dark Patterns in Websites/Web forms.....	13
2.4 List of the 25 Dark Patterns as extracted and compiled by the literature	15

2.1 Introduction

The increasing reliance on web platforms for everyday activities has led to the large-scale collection and processing of personal data. As users interact with digital services, they are frequently required to disclose personal information through various interfaces. This has raised significant concerns regarding privacy, transparency, and user control over personal data in online environments [1].

This chapter introduces the key concepts necessary for understanding these challenges. It first presents the fundamental aspects of privacy and personal data protection in web platforms, followed by an examination of how personal data are collected and processed through online interfaces. It then discusses the regulatory framework governing these practices, with a particular focus on the General Data Protection Regulation (GDPR) and its core principles. Finally, the chapter introduces the concept of dark patterns, highlighting how interface design can influence user decisions and affect the way personal data are disclosed and managed. Then, related work is presented in regards to collection and processing of personal data in the website more broadly, and then in specifics in regards to dark patterns in websites.

The remainder of this chapter is structured as follows. Section 2.1 introduces the study and its objectives. Section 2.2 presents the background of the research. Specifically, Section 2.2.1 introduces privacy and personal data protection in web platforms. Section

2.2.2 discusses the regulatory and legal context, focusing on the General Data Protection Regulation (GDPR) and its key principles. Section 2.2.3 introduces dark patterns and their role in influencing user decision-making in privacy-related interfaces. Section 2.3 reviews related work, with Section 2.3.1 covering works on the collection and processing of personal data on web platforms and Section 2.3.2 addressing works on dark patterns in websites and web forms. Finally, Section 2.4 provides a list of the 25 dark patterns as extracted and compiled from the literature.

2.2 Background

2.2.1 Privacy and Personal data protection in web platforms

Privacy has become one of the most important issues in modern digital society. In the context of online environments, privacy generally refers to an individual's ability to control how their personal information is collected, used, and shared by digital platforms and online services [1]. As internet technologies, software systems, and connected devices increasingly shape everyday activities, the amount of personal data generated and processed online has grown significantly. Consequently, concerns about the protection of personal data have become more prominent [1]. Privacy is therefore not only about keeping personal information hidden, but also about ensuring that individuals maintain meaningful control over how their information is accessed, processed, and distributed by digital services.

Personal data collection in web platforms occurs through a variety of user interactions and embedded technical mechanisms. In most cases, data are collected directly from users during their interaction with web interfaces, making the collection stage a central component of the user experience.

One of the primary methods of personal data collection is through web forms. These forms are commonly used in processes such as account registration, login authentication, newsletter subscriptions, contact requests, and online transactions. Through these interfaces, users may be asked to provide personal information including their name, email address, phone number, date of birth, and payment details. In many cases, the provision of such data is required in order to access or use a service, making data disclosure a necessary step in the interaction flow.

Once collected, personal data are processed for various purposes, including user authentication, service personalization, performance improvement, and targeted advertising. However, it is important to emphasize that the collection phase represents the primary point at which users are exposed to data-related decisions. The way in which data requests are presented through web interfaces can significantly influence user behavior and their willingness to disclose personal information, making data collection practices a critical aspect of privacy in web environments.

2.2.2 Regulatory and legal context (GDPR and related principles)

The extensive collection and processing of personal data by modern digital platforms has led to the development of regulatory frameworks aimed at protecting individuals' privacy and personal information. Within the European Union, the protection of personal data was initially addressed through the Data Protection Directive (DPD), which aimed to harmonize data protection standards across Member States and facilitate the free flow of personal data within the European market. However, as an EU directive, the DPD required implementation through national legislation, which resulted in inconsistencies in how data protection rules were applied across different countries.

To address these limitations and provide a more unified framework for personal data protection, the General Data Protection Regulation (GDPR) was adopted in 2016 and became fully applicable on 25 May 2018. Unlike directives, EU regulations apply directly in all Member States, ensuring a more consistent and harmonized approach to data protection across the European Union. The GDPR establishes comprehensive rules governing how organizations collect, process, and store personal data, applying not only to organizations within the EU but also to those outside the EU that offer services to individuals located in the European Union.

A key requirement of the GDPR is that organizations must provide clear and accessible information regarding the collection and processing of personal data. The regulation introduces several fundamental principles that guide how personal data should be handled. One of the most important principles is the Purpose Limitation Principle (Article 5(1)(b)), which requires organizations to clearly specify the purpose for which personal data are collected and how they will be used. Additionally, the GDPR emphasizes transparency (Article 12), requiring websites and online services to communicate their

data practices in a clear and understandable manner so that users can make informed decisions about their personal information.

Despite these regulatory requirements, many digital platforms still fail to effectively communicate how personal data are collected and processed[1]. As a result, users may not fully understand how their personal information is used by online services, which can lead to misunderstandings, potential compliance issues, and reduced user trust. Further to that, dark patterns is a technique used in websites to disorient users and lead them to proceed with actions, without full transparency or awareness this can also involve privacy-related actions.[2]

2.2.3 Dark Patterns

The term dark patterns was first introduced in 2011 by Harry Brignull [3], who launched the website darkpatterns.org in order to document and expose manipulative design practices used in digital interfaces. Brignull defined dark patterns as “tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something” [3]. The website originally known as darkpatterns.org has since been renamed to deceptive.design, reflecting the broader focus on deceptive interface practices and manipulative design techniques. In recent years, awareness of dark patterns has grown significantly across several research fields, including Human–Computer Interaction (HCI), computer science, and legal studies.

Several regulatory bodies have also addressed the issue of dark patterns in the context of data protection. For example, guidelines from data protection authorities define dark patterns as:

“In the context of these Guidelines, ‘dark patterns’ are considered as interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. Dark patterns aim to influence users’ behaviour and can hinder their ability to effectively protect their personal data and make conscious choices. Data protection authorities are responsible for sanctioning the use of dark patterns if these breach GDPR requirements.” [2]

Within the domain of privacy, dark patterns refer to interface design choices that manipulate users' decision-making processes in ways that may be detrimental to their privacy while benefiting the service provider [4]. The goal of most dark patterns is to manipulate users into taking actions that are inconsistent with their actual preferences, rather than genuinely informing or supporting their decision-making [5]. Through such design practices, users may be influenced to share additional personal information, accept tracking technologies, or make choices that they might not have made under transparent and neutral interface conditions.

For example, dark patterns in privacy-related interfaces may appear in mechanisms such as pre-selected consent options, confusing privacy settings, or misleading cookie consent banners that encourage users to accept tracking technologies. In some cases, options that allow users to reject data collection may be hidden, less visible, or presented in a way that makes them difficult to locate. Such design strategies can influence users' choices and may lead them to share more personal information than they would have intended under transparent and neutral interface conditions.[4]

A more detailed working definition of dark patterns in privacy has been proposed in the literature. According to this definition, «A dark pattern in privacy is an interface design choice that manipulates the data subject's decision-making process in a way detrimental to their privacy and beneficial to the service provider.». This definition highlights several key elements. First, dark patterns materialize through interface design choices, meaning that they arise at the point where users interact with digital services, such as websites or applications. These design choices are not neutral, but rather reflect intentional decisions that can influence user behavior. Second, dark patterns involve the manipulation of the user's decision-making process, often by exploiting cognitive biases or information asymmetries. Third, such manipulation leads to outcomes that are detrimental to the user's privacy, typically by encouraging the disclosure of more or more sensitive personal data than intended. At the same time, these practices benefit service providers by increasing data collection, reinforcing existing power imbalances between users and data controllers.[4]

2.3 Related Work

2.3.1 Works on the collection and processing of personal data on web platforms

Prior research has identified challenges related to compliance with privacy control requirements on websites. For instance, early studies conducted by the Federal Trade Commission (FTC) found that privacy control mechanisms were not consistently implemented, with only 61% of surveyed websites providing users with options regarding the collection of their personal information. More recent research has also revealed cases of non-compliance with the General Data Protection Regulation (GDPR). For example, some major websites have been shown to deliver targeted advertisements to European users even when they did not provide consent for the processing of their personal data[6].

For example, Habib et al. in “An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites” investigated how mechanisms such as email opt-out options, targeted advertising controls, and data deletion requests are implemented within web interfaces and privacy policies. The findings show that although many websites provide mechanisms intended to give users control over their personal data, these controls are often difficult to locate, inconsistently implemented, or poorly explained. In several cases, privacy choices were embedded in complex privacy policies or contained incomplete information about how the mechanisms function. These usability and transparency issues may limit users’ ability to effectively understand and manage how their personal data is collected and processed[6].

Another line of research has examined whether websites comply with the requirements introduced by the General Data Protection Regulation (GDPR). For instance, Matte et al. in “Do Cookie Banners Respect My Choice?”[7] analyzed how cookie consent banners on websites implement GDPR requirements regarding user consent and data collection transparency. The study evaluated a large number of websites and found that many cookie consent interfaces do not fully comply with GDPR principles, particularly regarding informed and freely given consent. In several cases, cookie banners were designed in ways that encouraged users to accept tracking technologies while making rejection options less visible or more difficult to access. These findings highlight significant challenges in the practical implementation of GDPR requirements within web interfaces

and raise concerns about whether users are able to make truly informed privacy decisions[7].

One example of a tool designed to assist users in understanding privacy practices is PriX (Privacy Policy eXplainer), introduced by Brunotte et al. in their paper “What About My Privacy? Helping Users Understand Online Privacy Policies.”[8] The purpose of this tool is to support end-users in dealing with privacy policies by providing contextual information in a more user-friendly and understandable manner, thereby improving users’ privacy awareness. PriX operates through three main steps: first, it checks whether a website provides a privacy policy; second, it analyzes the content of the privacy policy; and third, it provides visual explanations that help users better understand the information contained in the policy. Results from the user study showed that 88% of the participants agreed that the visual explanations provided by PriX helped them better understand the presented privacy information, demonstrating the potential of such tools to enhance users’ understanding of privacy-related practices[8].

Another tool aimed at improving transparency in data collection interfaces is presented in the work of Anna’s Vasileiou “Making Data Collection Transparent, Usable & GDPR-Compliant: Annotating Web Forms with Processing Purposes.” In this work, the author designed and developed the Privacy Annotation Tool, a browser-based application intended to support privacy-aware web form design. The tool enables users, particularly web developers, designers, and legal experts, to add privacy-related explanations directly to HTML form fields. These annotations provide contextual information about how personal data are processed, helping improve transparency and user trust. The explanations can be integrated into the form interface through selectable styles, such as short descriptions or information icon pop-ups, allowing them to be smoothly incorporated into existing website layouts.

These studies, even though addressing important topics, they overlook the existence of dark patterns in such interfaces, and mainly focus on making privacy policies or regulatory text on collection forms less complicated for the users to understand.

2.3.2 Works on Dark Patterns in Websites/Web forms

Several studies emphasize that research on dark patterns does not converge on a single definition or concern, but instead encompasses a set of thematically related perspectives, drawing on insights from psychology, economics, ethics, philosophy, and law. [9] However, despite this rich theoretical foundation, dark patterns are often embedded in everyday web interfaces in ways that are not immediately apparent to users.

In the study *Dark Patterns in Personal Data Collection: Definition, Taxonomy, and Lawfulness*, Luiza Jarovsky (2022)[4] examines dark pattern practices as a significant challenge to privacy and data protection law, with a particular focus on the European Union legal framework and the GDPR. The author approaches dark patterns from a legal and behavioral perspective, proposing a clear definition and distinguishing them from benign nudging practices, while analyzing the cognitive biases they exploit in the context of personal data processing. Furthermore, the study develops a taxonomy of dark pattern practices and evaluates their lawfulness under existing EU data protection principles. By comparing different models of user decision-making, the article highlights the limitations of current legal approaches and explores regulatory avenues for effectively preventing and prohibiting manipulative data collection practices.

Estelle Herbiet (2025) provides a regulatory and legal analysis of dark patterns in her master's thesis, "Dark Patterns and Privacy Rights in the Digital Age: Evaluating the GDPR and DSA's Regulatory Responses to Deceptive Designs"[10]. The thesis examines how dark patterns are addressed within the European Union legal framework, with particular emphasis on the interaction between the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). Herbiet evaluates the effectiveness and limitations of these regulatory instruments in tackling deceptive design practices, highlighting gaps stemming from the GDPR's indirect applicability to dark patterns and the DSA's reliance on future guidance and enforcement mechanisms. Furthermore, the thesis assesses whether the current fragmented regulatory landscape provides adequate protection for user privacy and autonomy, and proposes a more unified and targeted regulatory approach to improve legal certainty, enforcement, and harmonization in addressing dark patterns within the EU.

Empirical evidence on the effects of dark patterns has been provided by Francisco Lupiáñez-Villanueva, Alba Boluda, Francesco Bogliacino, Giovanni Liva, Lucie Lechardey, and Teresa Rodríguez de las Heras Ballell (2022) in their “Behavioural study on unfair commercial practices in the digital environment”[11]. The authors examine the prevalence and nature of dark patterns and manipulative personalisation within the European Union, focusing on their impact on consumer decision-making, autonomy, and vulnerability. By employing a combination of behavioural, psychological, and neurophysiological methods, the study demonstrates that such practices can significantly distort user choices and reinforce power asymmetries between digital service providers and users. Furthermore, the authors assess the adequacy of existing EU consumer and data protection frameworks, highlighting limitations in enforcement and transparency-based regulatory approaches, and propose policy-oriented recommendations to address these challenges.

A normative and conceptual foundation for understanding dark patterns is developed by Arunesh Mathur, Jonathan Mayer, and Mihir Kshirsagar (2021) in the study “What Makes a Dark Pattern... Dark?”[9]. The authors seek to move beyond purely descriptive accounts of dark patterns by examining why certain interface designs are problematic for users and society, addressing the absence of a unified definition in existing literature. Through a critical synthesis of prior research, the study argues that dark patterns are grounded not in a single concern but in a set of thematically related normative issues. Drawing on interdisciplinary perspectives from human–computer interaction, psychology, economics, ethics, philosophy, and law, the authors propose a set of normative lenses that can be used to systematically analyze and evaluate dark patterns and their broader societal implications. The study ultimately provides a framework to guide future empirical research, design practice, and policy-making related to the assessment and regulation of deceptive interface designs.

Most of the related work found in the literature on dark patterns originates from disciplines such as sociology and psychology. However, no study has examined this issue from the perspective of computer science or proposed technical infrastructures and solutions to address it. This gap is what the present work aims to bridge.

At the same time, studies that identify dark patterns specifically in registration forms and account-related pages are relatively dated, with most of them published around 2018. Therefore, the present study contributes an updated list of dark patterns based on an analysis of contemporary real-world web interfaces.

2.4 List of the 25 Dark Patterns as extracted and compiled by the literature

Based on the review of the literature presented in the previous sections, a set of dark pattern practices was identified and compiled from multiple research sources. These studies provide various definitions, taxonomies, and categorizations of manipulative interface design practices used in digital platforms. By examining these contributions, the most frequently referenced and conceptually relevant dark patterns were extracted and synthesized into a consolidated list.

The resulting list consists of 25 dark patterns, which represent common manipulative design practices identified across prior studies. This list serves as the analytical framework for the present research and it is used in the manual audit of websites conducted in this study and presented in Chapter 3, as well as for the taxonomy created and presented in Chapter 4, which will then serve as input in the software tool developed (Chapter 6). Each pattern represents a specific interface strategy that may influence user decision-making regarding privacy, consent, or the disclosure of personal information.

The compiled list of dark patterns used in this research is presented below.

1.Bad Defaults: The default options are sometimes chosen badly in the sense that they ease or encourage the sharing of personal information.

2.Hidden legalese stipulations: Services hide stipulations in the policies which target the privacy of the user.

3.Ease: when a user interface focus on the positive aspects of one choice while glossing over any potentially negative aspects inclining many users to comply with the service provider's wishes.

4.Impenetrable wall: is a user interface that “ block the access to a service with a cookie wall or account creation when that is not necessary to user the service “ .

5.Last minute consent: involves “seeking consent for the collection of data at a specific moment where we know that the individual is in a weak position because they are in a hurry or impatient to finish.

6.Pressure to allow permissions: not allowing the use of a service unless multiple permissions are conceded (i.e, access to the camera , microphone , gps).

7.Pressure to receive marketing: requiring the data subject to check the box “ receive marketing offers per email” to conclude a purchase or sign up.

8.Pressure to confirm: using negative persuasive language to make a data subject feel bad about not accepting a certain modality of data collection (i.e., a op-up window in an e-commerce site that shows two buttons, one saying “yes I want to create a login to gain access to the best offers” and the other saying “no , I do not like offers , I prefer paying a higher price)

9.Difficult deletion: making it difficult (i.e., having to correctly navigate through multiple drop-down choices) or inconvenient (i.e., requiring the data subject to speak with a representative through the phone) to delete the account , occasioning continuous data collection.

10.Hidden settings: hiding privacy settings in a places that is not intuitive or that the data subject needs to correctly navigate through multiple drop-down choices to arrive.

11.Ambiguity: using confusing language such as in a pop-up stating “do not share my data with third parties” with the options “yes” and “no” . It is unclear if “yes” means “share” or “do not share”.

12.Twist: using colors and symbols in a way that is different than what is customary to misguide the data subject (i.e. using green in the “deny” and red in the “accept” button)

13.Obfuscation: adding elements to a privacy setting that are not connected to privacy , so that privacy information get obfuscated.

14.Bad visibility: using badly contrasted , light colors or small fonts to make privacy-protecting options less visible.

15.False necessity: describing privacy-invasive features in a positive way to distract data subject from their downsides.

16.Forced registration: customer tricked into thinking registration is necessary.

17.Nagging: Given a choice between signing up for notifications , with the only options presented being “Yes” and “Not Now” , only to being asked again about signing up for notifications two weeks later when you select “Not Now” .

18.Continuous prompting: where users are persistently requested data or authorizations for new users of their personal data. The constant interruptions can lead to user fatigue , causing them to relent and provide more personal information or accept data uses they might otherwise reject.

19.Conflicting information: a method where users are presented with contradictory information , leading to confusion and inaction , often resulting in users defaulting to pre-set possible invasive settings.

20.Friend spam: Manipulative extraction of information about other users.

21.Language Discontinuity: when , despite the service being offered in the official language(s) of the country where users reside , the data protection related information is not provided in those languages . This disconnect prevents users from fully understanding how their personal data is processed or how to exercise their rights.

22.Immortal accounts: Account and consumer information cannot be deleted.

23.Privacy invasive defaults: privacy-invasive defaults (i.e., a video social network app that shares videos publicly by default)

24.Too many options method: overwhelms users, leading to too many options method overwhelms users, leading to decision paralysis or accidental oversight of critical settings related to their data protection preferences or rights.

25.Account Registration: no consent checkbox is provided, i.e., agreement is implied

Chapter 3

Dark Patterns in privacy collections UIs – the current web landscape

3.1 Introduction.....	19
3.2 Data Collection	19
3.3 Results	24
3.3 Conclusion	34

3.1 Introduction

This chapter presents the systematic investigation that we conducted on dark patterns in privacy-related web interfaces through a structured manual audit. The study focuses on how interface design influences user decisions during key interaction points, i.e., where websites collect and manage personal data.

The methodology is based on a carefully constructed dataset of widely used websites, combined with a detailed auditing process that examines multiple interface surfaces, including home pages, registration flows, settings, and account management features. Each identified case is recorded and categorized according to our predefined list of dark patterns (as presented in Chapter 2.3), enabling a structured analysis of their occurrence and distribution.

The results provide a comprehensive overview of how dark patterns appear across website categories, interface surfaces, and individual platforms. By analyzing both their frequency and placement, this chapter aims to highlight recurring design practices that influence user behavior and shape privacy-related decisions in the current web environment, and collect data towards the creation of a standardized taxonomy (Chapter 4).

3.2 Data Collection

To examine the presence of dark patterns in privacy-related web interfaces, a manual audit was conducted on a sample of $n=81$ popular websites. The purpose of this process was to explore how users are guided or influenced when making decisions related to their personal data.

The first step of the process was the selection of the websites to be audited. For this purpose, a list of the 100 most visited websites was compiled using publicly available rankings[12][13]. These sources were used in order to construct a sample consisting of highly popular and widely used websites, which are more likely to reflect the current privacy experience of everyday internet users. After collecting the websites, they were grouped into categories. The categorization was based on online activity categories inspired by [14], ensuring that the sample covers a broad range of commonly performed online activities.

The resulting categories are the following:

- Finding news about goods and services (21 websites)
- Buying/Ordering goods and services online (18 websites)
- Participating in Social Networks (15 websites)
- Communication (12 websites)
- Reading online news and newspapers (12 websites)
- Online Banking(3 websites)

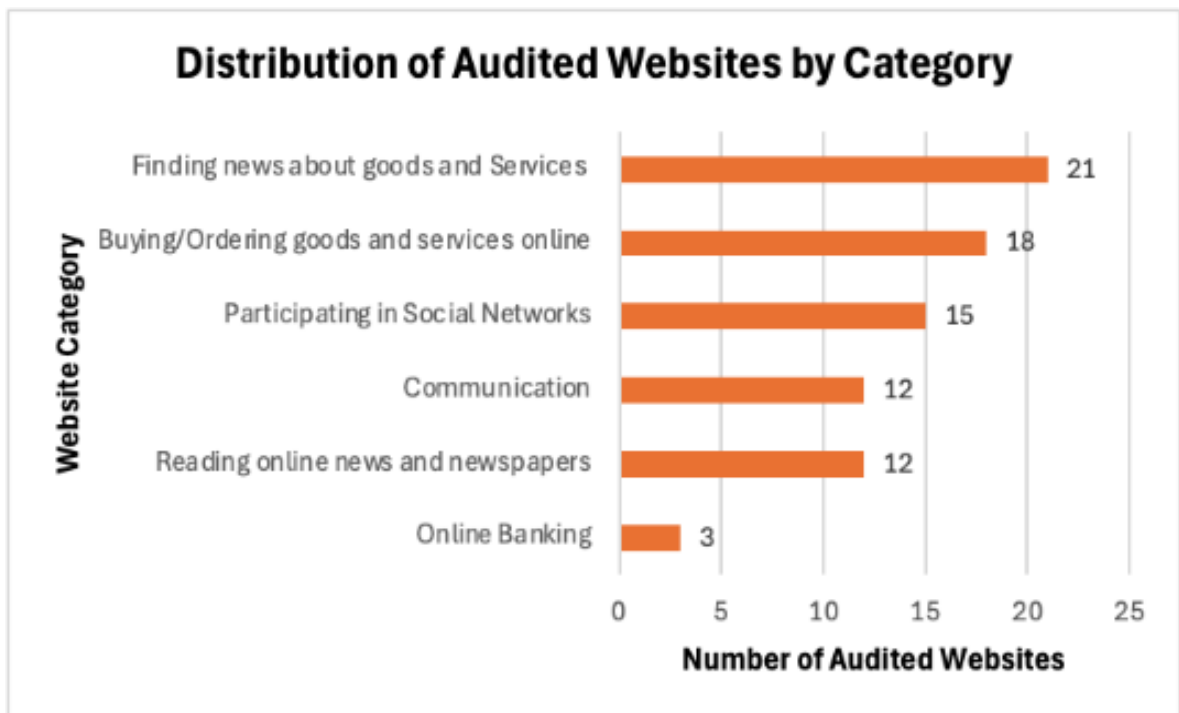


Figure 3.1: Distribution of Audited Websites by Category

The distribution of the audited websites across categories is presented in Figure 3.1. The results show that the largest portion of the sample falls under the category “Finding news about goods and services” (21 websites), followed by “Buying/Ordering goods and services online” (18 websites) and “Participating in social networks” (15 websites). The categories “Communication” and “Reading online news and newspapers” are equally represented with 12 websites each, while “Online Banking” includes a smaller subset of 3 websites.

Overall, the distribution indicates that the dataset is not dominated by a single category, but instead provides a relatively balanced representation of different types of online activities. This supports the objective of capturing a broad view of how dark patterns appear across diverse web contexts.

Although the initial dataset was based on a list of the 100 most visited websites, the final audited sample consists of 81 websites. This reduction occurred because certain websites appeared in multiple regional or language-specific versions (e.g., domain variations such as different country extensions), and in some cases, specific versions were excluded due to accessibility or language limitations that prevented consistent evaluation. As a result, only one representative version of such websites was included, ensuring consistency and comparability across the audit.

After the website list and categories were finalized, the manual audit was carried out individually for each website. The auditing process followed a consistent but exploratory procedure. First, the home page of each website was examined, with particular attention given to the cookie banner, as this is often the first point at which users are asked to make privacy-related decisions. The evaluation focused on the design and presentation of consent mechanisms, aiming to identify interface characteristics that may guide or influence user choices.

Next, an attempt was made to create a user account on the website whenever this was possible. During this step, the registration flow was examined in order to identify dark patterns related to personal data entry, consent requests, pre-ticked boxes, forced

disclosure, or implied agreement to privacy-related terms. After registration, the account settings and any available privacy or security settings were reviewed to assess how personal data controls were presented to users and whether privacy-protective options were accessible, transparent, or intentionally obscured.

Finally, an attempt was made to delete the created account, in order to examine the account deletion flow and identify any friction, hidden navigation paths, discouraging wording, or other design decisions that made deletion unnecessarily difficult. Since each website had a different structure and user journey, the auditing process was not limited only to predefined pages. In cases where a tab, button, or section appeared likely to contain privacy-relevant or potentially manipulative interface elements, it was also visited and examined. This allowed the audit to remain flexible enough to capture dark patterns appearing outside the main expected surfaces.

Based on this procedure, the main interface surfaces examined during the audit included the home page, registration/sign-up page, login page, settings page, privacy settings, security page, help/support pages, and account deletion flows. These surfaces were selected because they are common points where websites collect, process, or manage personal data. More specifically, the home page was important mainly because of cookie banners and initial consent requests, registration and sign-up pages were examined because they explicitly collect personal information through forms and consent fields, settings, privacy, and security pages were relevant because they often contain user controls related to data sharing, personalization, advertising, and account visibility, and account deletion or help/support pages were inspected because they frequently reveal whether websites make data withdrawal and account removal straightforward or intentionally difficult.

The selected interface surfaces were not arbitrary, but were chosen because they represent common points of interaction through which websites collect, request, manage, or retain personal data. Registration and sign-up pages are primarily used to collect personal information required for account creation, such as names, email addresses, passwords, phone numbers, or birth dates. Home pages are particularly important because they often display cookie banners and initial consent notices related

to tracking and data processing. Settings, privacy, and security pages are relevant because they provide access to user controls concerning visibility, personalization, advertising, data sharing, and account protections. Finally, account deletion and support pages are critical for evaluating whether users are given a clear and fair opportunity to withdraw from the service and remove their personal data.

Table 3.1 summarizes the above interface surfaces, the reason they were selected, and the specific points examined in each.

Interface Surface	Why Selected	Examined Points
Home Page	Initial user entry	Cookie banners, consent UI, defaults
Registration / Sign-up	Data collection point	Form inputs, pre-ticked boxes, forced consent
Login Page	User re-entry	Tracking prompts, hidden consent
Account Settings	User control center	Data visibility, accessibility
Privacy Settings	Data management	Options clarity, granularity
Security Settings	Data protection	Security features, user control
Help / Support	Indirect access	Hidden paths, navigation
Account Deletion	Data removal	Steps, friction, discouragement

Table 3.1: Interface Surfaces Examined During the Manual Evaluation Process

All audit observations were systematically recorded in an Excel spreadsheet. Each row in the spreadsheet represented one identified dark pattern instance on a specific website interface. The spreadsheet included the following columns:

- (A) Website Domain, referring to the main domain of the audited website
- (B) Website URL, indicating the exact page where the dark pattern was identified
- (C) ID of Dark Privacy Pattern, according to the dark patterns list developed earlier in this study (Chapter 2.4)
- (D) Category of Website, indicating the functional category to which the website belonged

(E) Surface, referring to the specific interface location where the dark pattern appeared, such as Registration Page, Home Page, or Settings Page

(F) Description, a short text description with observations about the specific dark pattern in the specific website and surface.

Manual audit of dark patterns across popular websites (2025)		
Website URL	Number of Dark Pattern (According to th Category of Website	
https://www.microsoft.com/el-gr/microsoft-365/	3	Communication
https://www.microsoft.com/el-gr/microsoft-365/	2	Communication
https://www.fandom.com/	24	Finding news about goods and Services
https://www.fandom.com/	10	Finding news about goods and Services
https://www.fandom.com/	2	Finding news about goods and Services
https://www.fandom.com/	14	Finding news about goods and Services
https://www.fandom.com/	13	Finding news about goods and Services
https://auth.fandom.com/register?flow=386898	7	Finding news about goods and Services
https://community.fandom.com/wiki/Special:Clk	9	Finding news about goods and Services
https://www.msn.com/en-xl	24	Reading online news and newspapers
https://www.msn.com/en-xl	2	Reading online news and newspapers
https://www.msn.com/en-xl	13	Reading online news and newspapers
https://www.netflix.com/signup?serverState=%	7	Buying/Ordering goods and services online
https://www.pinterest.com/	3	Participating in Social Networks
https://policy.pinterest.com/el/cookies	2	Participating in Social Networks
https://www.pinterest.com/login/?message=acc	9	Participating in Social Networks
https://mail.ru/	1	Communication
Surface	Description	
Home page	The cookie banner emphasizes positive outcomes such as "improving user experience" while downplaying the implications of personalized advertising and tracking.	
Home page	References to third-party cookies are included in the cookie notice but require additional navigation to access meaningful details.	
Home page	The consent interface overwhelms users by presenting hundreds of partners and multiple processing purposes, making informed decision-making impractical.	
Home page	Refusing or limiting consent requires navigating through multiple layers (purposes and partner lists), significantly increasing user effort.	
Home page	Sensitive data processing practices (e.g. precise geolocation and device identification) are disclosed within dense legal text rather than clearly highlighted.	
Home page	The accept button is different colour from the other button	
Home page	Multiple data processing purposes and actors are grouped together without clear separation, reducing transparency.	
Registration Page	The registration form includes a preselected checkbox for receiving marketing emails, nudging users into consenting unless they actively opt out.	
Help Page	Had to navigate to multiple pages in order to delete my account.	
Home page	The consent interface overwhelms users by referencing 852 partners and multiple processing purposes, making informed consent impractical.	
Home page	Highly intrusive data processing practices are disclosed within dense informational text without adequate prominence or contextual explanation.	
Home page	Multiple processing purposes and third-party actors are grouped together, reducing clarity about how and by whom personal data is processed.	
Registration Page	Marketing emails are enabled by default through an opt-out checkbox framed with negative wording ("Please do not email me"), nudging users to accept marketing communications.	
Home page	The cookie banner emphasizes personalization and improved user experience while downplaying the privacy implications of tracking and advertising cookies.	
Privacy Policy Page	Information about third-party technologies and data collection is disclosed only within the cookie policy layer rather than at the initial consent interface.	
Settings Page	Account deletion requires additional steps outside the main interface (email-based confirmation), introducing friction compared to the significantly simpler registration process.	
Home page	The option to manage privacy settings is visually de-emphasized compared to the prominent "Accept all" button.	

Figure 3.2: Manual Audit of dark patterns across popular websites(2025)

In addition to the spreadsheet, screenshots were captured for every identified case of a dark pattern. These screenshots were then organized in a separate Word document, allowing each observation in the dataset to be linked to visual evidence. This step was important both for documentation and for improving the reliability of the audit, since each recorded observation was supported by a corresponding interface capture and a short explanatory note.

3.3 Results

The results of the manual audit provide insights into the prevalence and distribution of dark patterns across different types of websites and interface surfaces. This section presents the findings through a series of graphs, each highlighting a different aspect of the collected data. The analysis focuses on identifying the most common dark patterns,

their distribution across website categories and interface surfaces, and the extent to which multiple dark patterns co-exist within individual websites.

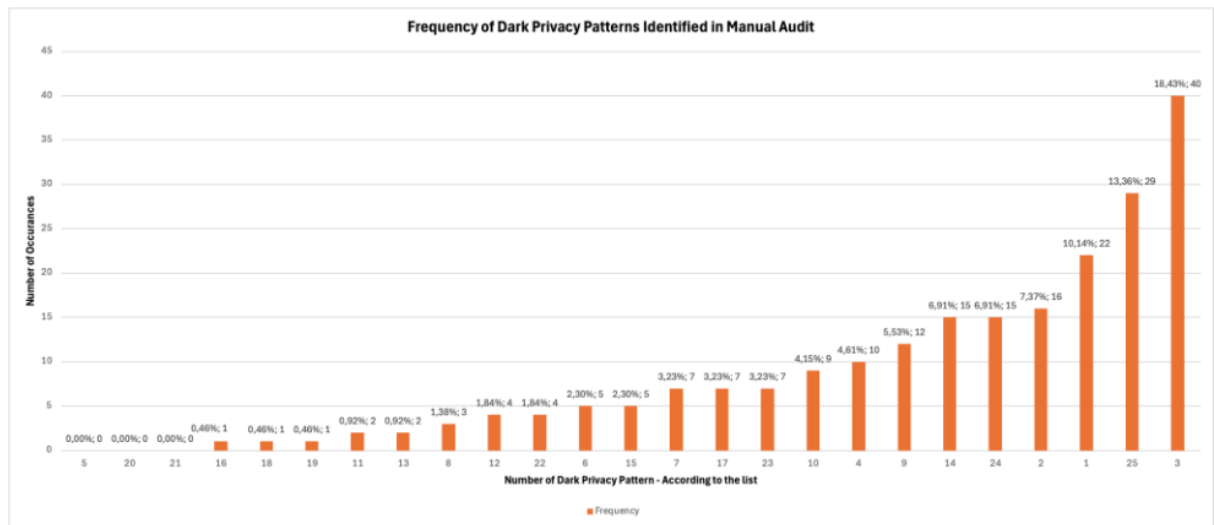


Figure 3.3: Frequency of dark privacy patterns identified in the manual audit (sorted by occurrence)

Figure 3.3 presents the frequency of each dark pattern identified during the manual audit. The results show that Dark Pattern 3 (Ease) is the most frequently observed, with 40 occurrences (18.43%), followed by Dark Pattern 25 (Account Registration) with 29 occurrences (13.36%) and Dark Pattern 1 (Bad Defaults) with 22 occurrences (10.14%). Other patterns, such as Dark Pattern 2 (Hidden legalese stipulations), Dark Pattern 14 (Bad visibility), and Dark Pattern 24 (too many options method), also appear relatively frequently, with occurrences ranging between 15 and 16. In contrast, several patterns, including Dark Pattern 5 (Last Minute Consent), Dark Pattern 21 (Language Discontinuity), and Dark Pattern 20 (Friend spam), exhibit zero occurrences.

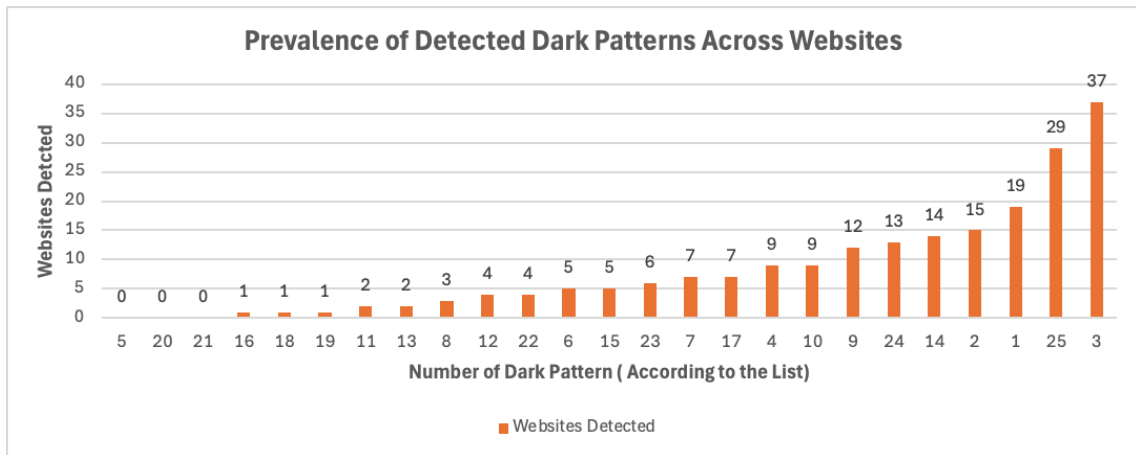


Figure 3.4 Prevalence of Detected Dark Patterns Across Websites

Figure 3.4 presents the prevalence of detected dark patterns across the evaluated websites. In contrast to the analysis presented in Figure 1, this graph illustrates in how many different websites each dark pattern was identified, rather than the total number of occurrences recorded during the manual audit. In this analysis, each dark pattern was counted only once per website, regardless of how many times it appeared within different pages or interface surfaces of the same platform.

The results show that Dark Pattern 3 (Ease) was the most prevalent pattern, appearing in 37 different websites, followed by Dark Pattern 25 (Account Registration), which appeared in 29 websites, and Dark Pattern 1 (Bad Defaults), which was identified in 19 websites. Other relatively common patterns included Dark Pattern 2 (Hidden legalese stipulations), Dark Pattern 14 (Bad visibility), and Dark Pattern 24 (Too many options), which also appeared across multiple platforms.

Compared to Figure 1, which measured the total number of dark-pattern occurrences across all analyzed interface surfaces, Figure X focuses on website-level prevalence. This distinction is important because a single website may implement the same dark pattern multiple times across different pages or interface components. Therefore, while Figure 1 illustrates the intensity and repeated implementation of dark patterns within platforms, Figure X demonstrates how widespread each dark pattern category was across the evaluated websites.

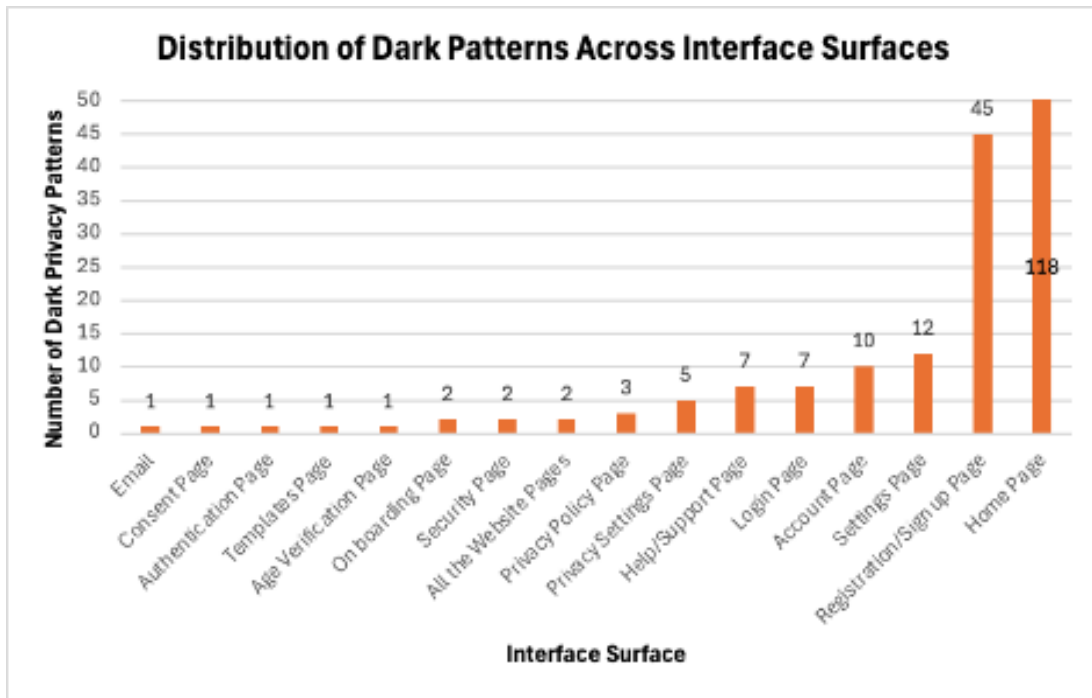


Figure 3.5: Distribution of dark patterns across interface surfaces

Figure 3.5 presents the distribution of dark patterns across different interface surfaces. The results show that the Home Page contains the highest number of dark patterns (50), followed by the Registration/Sign-up Page (45). A moderate number of occurrences is observed in the Settings Page (12) and the Account Page (10), while both the Login Page and the Help/Support Page include 7 occurrences each. Lower frequencies are recorded for the Privacy Settings Page (5) and the Privacy Policy Page (3), whereas several surfaces, such as Email, Consent Pages, Authentication Pages, and Template Pages, exhibit minimal presence with only one or two occurrences.

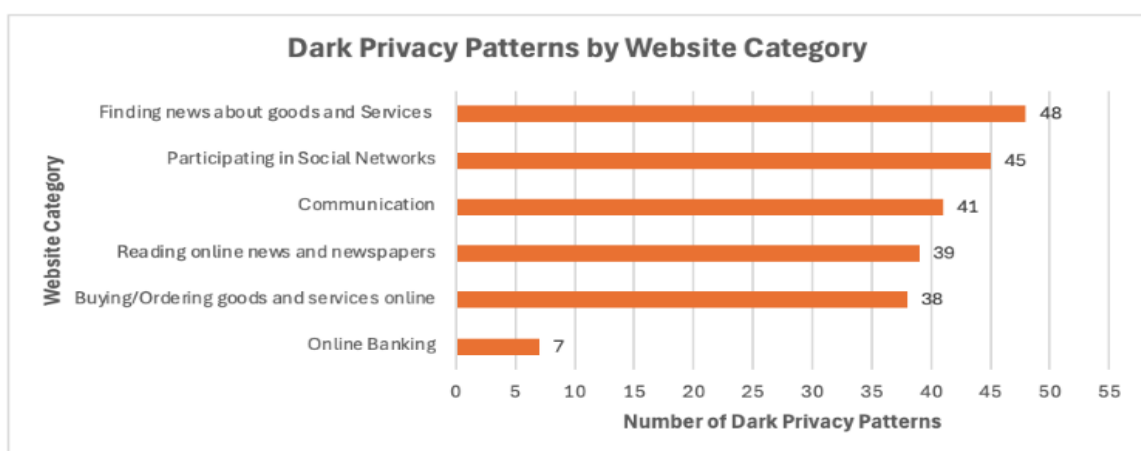


Figure 3.6: Dark Patterns by Website Category

Figure 3.6 presents the distribution of dark privacy patterns across different website categories. The results show that the highest number of dark patterns is observed in the category “Finding news about goods and services” (48), followed by “Participating in social networks” (45) and “Communication” (41). The categories “Reading online news and newspapers” (39) and “Buying/Ordering goods and services online” (38) also show similarly high numbers. In contrast, the “Online Banking” category contains significantly fewer dark patterns, with only 7 recorded instances.

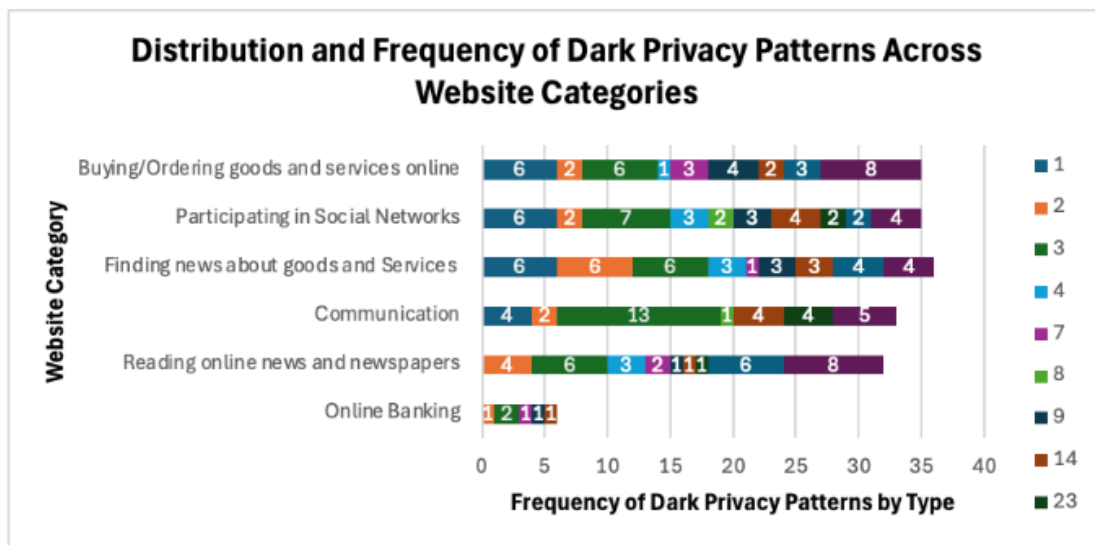


Figure 3.7: Distribution and Frequency of Dark Patterns Across Website Categories

Figure 3.7 presents the distribution and frequency of dark privacy patterns across different website categories. Each bar represents the total number of dark patterns identified within a specific category, while the individual segments within each bar correspond to different dark pattern types. The numbers displayed inside each segment indicate how many times each specific dark pattern appears within that category. For example, in the category “Buying/Ordering goods and services online”, a total of 35 dark patterns were identified, of which 6 correspond to Dark Pattern 1 (Bad Defaults).

It should be noted that not all dark pattern types are displayed in this figure. In order to maintain readability and clarity, only the most frequently observed dark patterns are included. Including all identified patterns would result in a visually complex and difficult-

to-interpret chart. Therefore, this visualization focuses on the most common patterns, which provide a clearer representation of the dominant trends across website categories.

Website	Dark Patterns Count
canva.com	8
dropbox.com	8
fandom.com	8
spotify.com	8
tripadvisor.com	8
mail.ru	8
theguardian.com	8
dailymotion.com	5
Wikipedia.com	5
discord.com	5
tumblr.com	5
paypal.com	5
aliexpress.com	4
steampowered.com	4
roblox.com	4
Yahoo.com	4
notion.com	4
etsy.com	4

dailymail.co.uk	4
adobe.com	3
rutube.ru	3
bbc.com	3
ikea.com	3
microsoft.com	3
imdb.com	3
marca.com	3
hbomax.com	3
twitch.tv	3
cnn.com	3
avito.ru	3
tiktok.com	3
fox.com	3
pinterest.com	3
msn.com	3
nytimes.com	2
Reddit.com	2
ya.ru	2
slack.com	2
X.com	2

asos.com	2
espn.com	2
github.com	2
claude.ai	2
primevideo.com	2
walmart.com	2
snapchat.com	2
ebay.com	2
globo.com	2
vimeo.com	2
Chatgpt.com	2
infobae.com	2
quora.com	2
threads.com	2
Facebook.com	2
indeed.com	2
ilovepdf.com	2
zoom.us	2
wise.com	1
dzen.ru	1
wildberries.ru	1

accuweather.com	1
vk.vom	1
bestbuy.com	1
uol.com	1
expedia.com	1
target.com	1
booking.com	1
soundcloud.com	1
netflix.com	1
shein.com	1
gemini.com	1
samsung.com	1
ecosia.org	1
revolut.com	1
cricbuzz.com	1
patreon.com	1
Bing.com	1
openai.com	1
Youtube.com	1
amazon.com	1
nike.com	1

Table 3.2: Dark Patters Identified per Website

Table 3.2 presents the number of dark patterns identified per website. The results show that most websites (n = 62) contain between 1 and 3 dark patterns, with a large portion of the sample concentrated in this range. A small portion of websites exhibit a higher number of dark patterns, reaching up to 7 (n = 4) or 8 (n = 2), representing the highest values observed in the dataset. Additionally, a group of n = 13 websites includes 4 to 6 dark patterns, indicating a moderate level of presence.

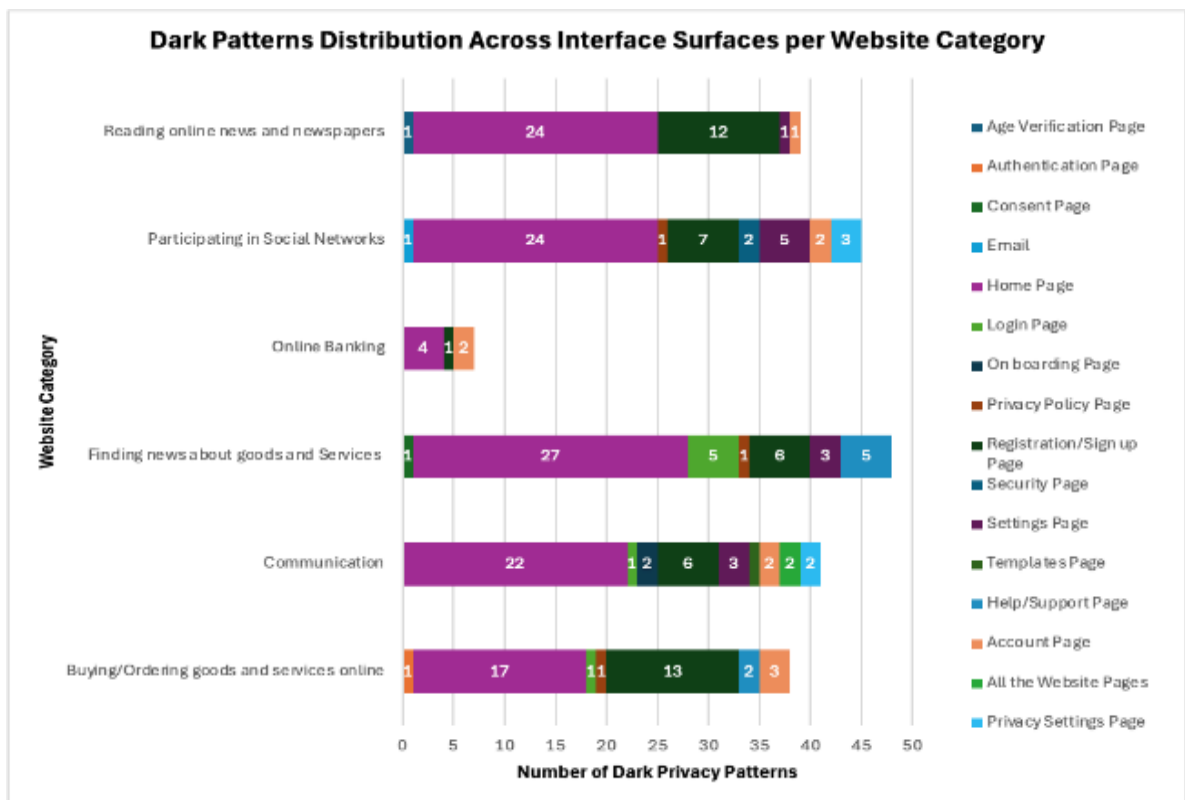


Figure 3.8: Dark Patterns Distribution Across Interface Surfaces per Website Category

Figure 3.8 presents the distribution of dark patterns across interface surfaces for each website category. Each bar represents a website category, while the segments within each bar correspond to different interface surfaces where dark patterns were identified. The numbers inside each segment indicate how many dark patterns were found on each surface within the specific category.

The results show that the Home Page contains the highest number of dark patterns across all categories, with particularly high values in “Finding news about goods and services”

(27), “Reading online news and newspapers” (24), and “Participating in social networks” (24). Additionally, the Registration/Sign-up Page and Login Page also show notable occurrences across several categories. In contrast, other surfaces such as Email, Authentication Page, and Privacy Policy Page appear less frequently.

3.3 Conclusion

The findings of the manual audit demonstrate that dark patterns are a systematic and widespread component of modern web interfaces. Rather than appearing as isolated cases, these patterns are consistently embedded across a large portion of the analyzed websites, often occurring multiple times within the same platform.

Chapter 4

A Taxonomy of Dark Patterns in Web Privacy	35
4.1 Introduction.....	35
4.2 Structure and Description of the Taxonomy	36
4.3 Human-readable format.....	39
4.4 Machine-readable format.....	40

4.1 Introduction

In order to systematically categorise dark patterns in web-based personal data collection and processing UIs, a structured taxonomy was developed. This taxonomy was developed following our extensive review of existing literature resulting in a compiled list of popular and important dark patterns (as presented in Chapter 2), regulatory guidelines background (e.g. GDPR), and our findings from the manual audit and analysis conducted and presented in Chapter 3.

A taxonomy provides a structured and systematic approach for organizing complex concepts into meaningful categories [15]. In the context of this research, it serves as a framework for identifying, categorizing, and analyzing dark patterns that influence users' decision-making processes related to personal data on the web.

The development of this taxonomy was guided by two main objectives. First, to provide a comprehensive and consistent way to describe dark patterns observed in modern web interfaces. Second, to enable the operationalization of these patterns in a way that supports their detection by automated or semi-automated tools, such as the one we present in Chapter 6.

The final presented taxonomy consists of 25 distinct dark pattern types, each defined based on a set of characteristics such as observable interface indications, and technical indicator. The taxonomy not only reflects theoretical definitions from prior work but mainly incorporates empirical observations from the manual audit, ensuring that it

accurately represents real-world practices and ensures that both auditing the interface and automated check of the code is supported.

4.2 Structure and Description of the Taxonomy

The proposed taxonomy is structured as a multi-attribute classification system that captures the characteristics of dark patterns related to personal data collection and processing in web environments. It consists of 25 distinct dark pattern entries, each described using a consistent set of fields.

Each dark pattern in the taxonomy is defined through the following attributes:

A) Dark Pattern number (according to the initial compiled list presented in Chapter 2.3): This field contains the numerical identifier of each dark pattern, based on the list presented in Chapter 2.4.

B) Dark Pattern Name: This field contains the name of each dark pattern according to the list in Chapter 2.3.

C) Dark Pattern Description: This field contains the description of each dark pattern, derived from existing literature.

The following fields about Interface Indicators capture the observable manifestation of dark patterns at different levels of the user interface. These indicators were derived from the conducted manual audit of real-world websites, focusing on how dark patterns appear to users through interface elements, placement, and interaction cues.

D) Typical Interface Location: This field indicates where each dark pattern typically appears within a web interface (e.g., cookie banners, registration forms, account settings).

E) Observable indications (What to look for): This field describes the observable characteristics that users can look for in a website in order to identify the presence of each dark pattern. It focuses on user-visible elements and interaction cues.

The following fields about Technical Indicators capture the technical implementation of dark patterns at different levels of the interface. These indicators were derived from the analysis of existing dark pattern implementations observed in real websites, where the source code was available.

F) Technical Indicators (DOM/HTML): This field includes implementation-level indicators related to the structure of the webpage (HTML/DOM) that can be used to identify each dark pattern.

G) Technical Indicators (CSS/Layout): This field includes visual and layout-related indicators that reflect how the interface design reinforces the dark pattern.

H) Technical Indicators (JavaScript/Behavior): This field includes behavioral indicators related to dynamic functionality and system logic that contribute to the presence of the dark pattern.

Additionally some other attributes are included:

I) Related GDPR Principles/Articles: This field links each dark pattern to relevant GDPR principles or articles that may be affected by its use. The mapping is based on the provisions of the GDPR, indicating how specific design practices may conflict with requirements such as transparency, fairness, and data protection by default.

J) Prevalence in Sample: This field indicates how frequently each dark pattern was observed during the manual audit.

K) Keywords: This field was derived from the conducted manual audit and captures keywords associated with each dark pattern, reflecting commonly used terms and phrases observed in real-world interfaces that may signal its presence and support its identification.

Figure 4.1 presents an extract of the proposed taxonomy illustrating key fields for selected dark patterns, including the pattern name, description, typical interface location, and

observable indications. This figure highlights how each dark pattern is systematically defined and identified by linking its conceptual characteristics with its common placement within the interface and its observable, user-facing manifestations, as derived from the conducted manual audit.

A	B	C	D	E
Taxonomy of Dark Patterns				
Number	Name of Dark Pattern	Description	Typical Interface Location (where it appears usually)	Observable Indications (What to look for)
1	Bad Defaults	The default options are sometimes chosen for the user		Check whether any options (e.g., cookies, marketing preferences, personalized features) are pre-selected by default
				Identify whether privacy-invasive settings (e.g., tracking, personalized advertising, data sharing) are enabled by default and require users to opt out
			Cookie banner Registration forms Account settings	Assess whether the interface favors data-sharing choices through visual emphasis (e.g., prominent "Accept all" option) or de-emphasized privacy settings Check whether users are required to take additional steps to disable data collection or refuse consent
2	Hidden legalese stipulations	Services hide stipulations in the policies w pages		Identify whether consent is implied (e.g., through continued use) or enforced due to the absence of a clear refusal option
				Check whether information about data collection, third-party sharing, or tracking is explicitly stated in the initial banner or interface, rather than only in linked policies
			Cookie banners Registration forms Account settings Privacy and cookie policy	Identify whether key details (e.g., use of third parties, personalized advertising, sensitive data processing) are accessible only through secondary links such as "Privacy Policy" or "Cookie Policy" Check whether important information is placed in low-visibility areas (e.g., footer links, small text below buttons, secondary layers) instead of the main consent interface Assess whether the language used is vague or non-specific (e.g., references to "partners," "other services," or "marketing purposes" without clear explanation)
				Identify whether users must navigate through multiple pages or clicks to understand how their data is collected, shared, or used

Figure 4.1: Extract of the proposed taxonomy

Furthermore, Figure 4.2 presents an extract of the proposed taxonomy illustrating the Technical Indicators for selected dark patterns, including DOM/HTML structure, CSS/layout properties, and JavaScript behavior, as well as their mapping to relevant GDPR principles, observed prevalence within the analyzed sample, and associated keywords. This figure highlights how dark patterns can be systematically identified by linking their technical implementation with regulatory context and empirical observations derived from the conducted manual audit.

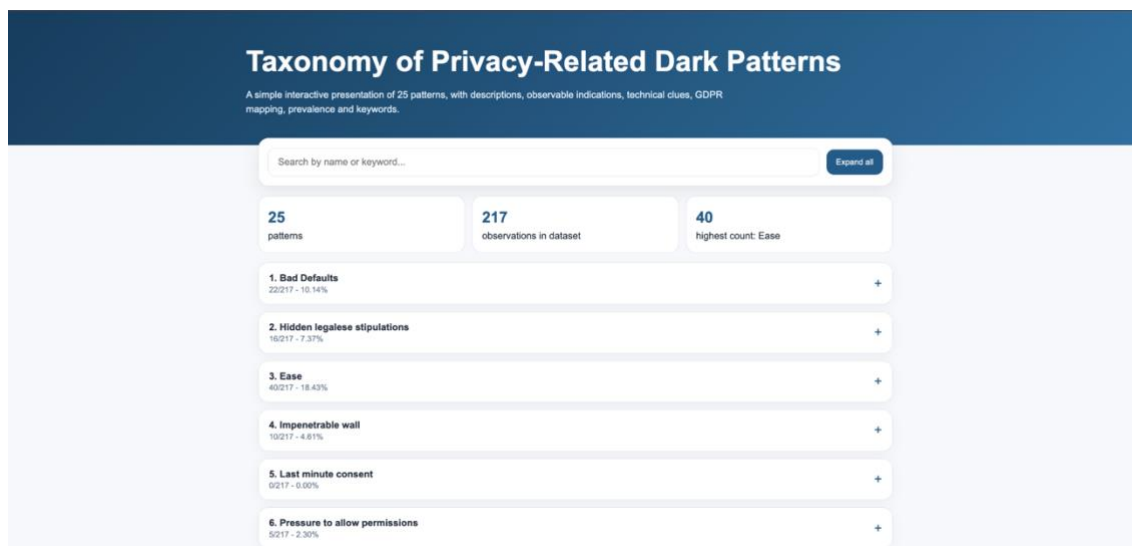


Figure 4.3: Taxonomy of Privacy – Related Dark Patterns I

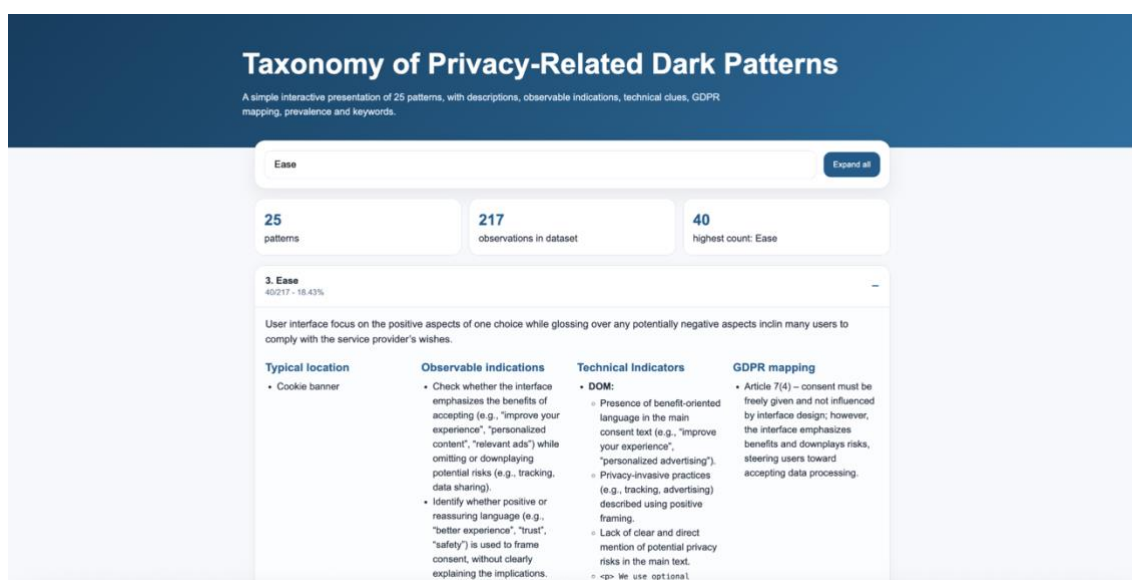


Figure 4.4: Taxonomy of Privacy – Related Dark Patterns II

4.4 Machine-readable format

In order to support the practical use of the proposed taxonomy, it was transformed into a structured, machine-readable format. Specifically, the taxonomy was translated in JSON format, allowing it to be directly integrated into software systems for the detection and analysis of dark patterns.

Each dark pattern in the taxonomy is represented as a structured JSON object, where each field corresponds to the attributes defined in Section 4.1. This representation preserves the structure of the taxonomy while enabling its direct use in computational processes. In particular, the JSON taxonomy is intended to serve as an input to the proposed detection

tool, forming the underlying knowledge base that supports the identification, interpretation, and analysis of dark patterns.

Another important advantage of the JSON representation is its extensibility. If new dark patterns are identified in the future, they can be added to the taxonomy without changing its overall structure. Similarly, additional attributes or updated indicators can be incorporated as needed. This makes the taxonomy flexible and ensures that the proposed tool can be continuously updated to reflect emerging dark pattern practices.

The JSON representation preserves the full structure of the taxonomy by including not only the conceptual description of each dark pattern, but also its observable indications, technical indicators, related GDPR provisions, and prevalence in the sample. This allows each pattern to be represented in a format that is both human-readable and machine-readable.

```
[
  {
    "patternNumber": 1,
    "name": "Bad Defaults",
    "description": "The default options are sometimes chosen badly in a way that favors personal data processing or sharing.",
    "typicalInterfaceLocation": [
      "Cookie banners",
      "Registration forms",
      "Account settings"
    ],
    "observableIndications": [
      "Check whether any options are pre-selected by default",
      "Identify whether privacy-invasive settings are enabled by default and require users to opt out",
      "Assess whether the interface favors data-sharing choices through visual emphasis",
      "Check whether users are required to take additional steps to disable data collection or refuse consent",
      "Identify whether consent is implied due to the absence of a clear refusal option"
    ],
    "technicalIndicators": {
      "domHtml": {
        "description": [
```

```

        "Presence of checkbox inputs with the checked
attribute enabled by default",
        "Data processing or preference options pre-
selected without user interaction",
        "Absence of explicit opt-in mechanism"
    ],
    "codeExamples": [
        "<input id=\"persistent\" name=\"persistent\"
type=\"checkbox\" checked>"
    ]
},
"cssLayout": {
    "description": [
        "Default-selected options are visually rendered as
active",
        "The checked state is reinforced through CSS
styling",
        "Privacy-protective alternatives are not equally
emphasized visually"
    ],
    "codeExamples": [
        "input[type=checkbox]:checked + label::before"
    ]
},
"javascriptBehavior": {
    "description": [
        "Default settings remain active unless the user
manually changes them",
        "No user action results in the default option
being applied",
        "The system behavior assumes acceptance unless the
option is explicitly deselected"
    ],
    "codeExamples": [
        "if
(document.getElementById(\"persistent\").checked) {
keepUserLoggedIn(); }"
    ]
}
},
"gdprMapping": [
    "Article 25(2) - data protection by default, personal
data processing and sharing should not be enabled by default"
],
"prevalence": {
    "count": 22,
    "total": 217,
    "percentage": 10.14
},
"keywords": [
    "checked",
    "pre-selected",
    "preselected",
    "enabled by default",

```

```
        "selected by default",  
        "default option",  
        "opt out",  
        "pre-ticked",  
        "ticked by default"  
    ]  
},
```

Chapter 5

Run the Study: “A user study on the effects of dark patterns in their consent decisions.”	44
5.1 Introduction.....	44
5.2 Data Collection	44
5.3 Results	47
5.3.1 Demographic Results.....	47
5.2.2 Background Information Results	49
5.2.3 Dark Patterns on the Web Results	51
5.4 Conclusion	68

5.1 Introduction

This chapter presents the user study conducted to evaluate users’ awareness, understanding, and perception of online practices in relation to dark patterns in privacy-related UIs, i.e., pages related to the collection of personal data. The primary objective of this study is to examine how effectively users recognize potentially manipulative design elements in such pages, and whether they are able to correctly interpret them.

To achieve this, an online questionnaire was designed and distributed to participants from diverse backgrounds (open call). The study incorporates both self-reported measures (such as perceived familiarity and confidence) and scenario-based evaluation, allowing for a more comprehensive assessment of user understanding and behavior.

The chapter is structured as follows: Section 5.2 describes the data collection process and the design of the questionnaire. Section 5.3 presents and analyzes the results of the study, supported by visualizations. Finally, Section 5.4 discusses the key conclusions derived from the findings.

5.2 Data Collection

The data for this study was collected through an online questionnaire developed using Google Forms. The survey was designed to capture user responses related to their

interaction with dark patterns in web interfaces and their ability to recognise and interpret them.

The questionnaire was structured into four main sections.

1) Demographic Information

The first section included questions related to participants' age group and field of study or work. This information is used to support potential comparisons across different user groups.

2) Background Information

The second section focused on participants' general use of the internet and their familiarity with digital environments. Participants were asked to indicate how frequently they use the internet, their familiarity level with digital technologies and online privacy, and whether they had prior knowledge of dark patterns.

3) Users Perception on Dark Patterns on the Web

In the third section, participants were initially presented with a short informational video titled "Short introduction about dark patterns". The video was created for the purposes of this thesis using the tool "Synthesia.io", and was used to introduce the concept of dark patterns and provide examples of common manipulative interface designs found in online environments.

This step was included to ensure that all participants had a basic understanding of the concept before proceeding with the rest of the questions. It also allowed the study to observe participant responses after exposure to explanatory content.

The following three questions were then presented to participants to assess their perception of dark patterns:

1. So far, when browsing the web, how often do you think you have been able to recognise and avoid dark patterns?
(Scale: 1 = Never, 5 = Always)
2. How confident do you feel in recognising and avoiding dark patterns?
(Scale: 1 = Not confident at all, 5 = Completely Confident)
3. Do you think a tool for recognising and avoiding dark patterns in websites would be useful?
(Scale: 1 = Not useful at all, 5 = Completely useful)

4) Scenario-based assessment

The final section included scenario-based questions presenting examples of common web interfaces that relate to personal data collection, such as cookie consent banners, registration forms, account deactivation processes, and subscription-related interactions.

For each scenario, participants were asked to respond to the following questions:

- Do you think anything in this screen is manipulative or misleading?
- If yes, where exactly do you notice it? If no, please write “N/A”.
- Why do you think it is manipulative, misleading, or unclear? If not applicable, please write “N/A”.
- How confident are you in your answer?

This section captures participant responses in a context that simulates real-world interaction with web interfaces.

Distribution and Sample

The questionnaire was distributed online through social media platforms and direct communication channels. Participation was voluntary and anonymous. Participants were informed by a brief text about this before giving consent to participate.

A total of 101 responses were collected and included in the analysis.

5.3 Results

5.3.1 Demographic Results

The majority of participants belonged to the 18–24 age group (62%), followed by participants aged 25–34 (27%). The remaining age groups represented a significantly smaller portion of the sample.

This indicates that the study primarily reflects the perspectives of younger and digitally active users, who are more likely to interact frequently with modern web platforms and online services.

What is your age group?

101 απαντήσεις

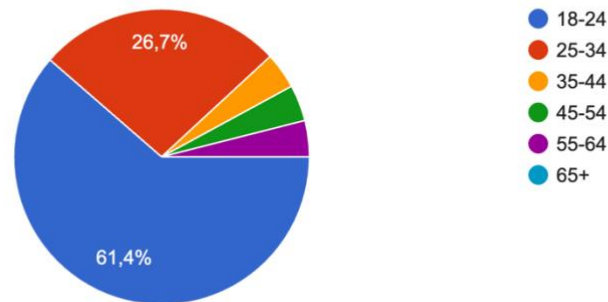


Figure 5.1: What is your age group?

Participants came from a variety of academic and professional backgrounds. Since the question was open-ended, participants described their academic or professional background using different terminology, even when referring to similar fields. As a result, the original graph became difficult to interpret, and the responses were therefore grouped into broader thematic categories and presented in tabular form to improve clarity and readability. For this reason, similar responses were grouped under a common category in the following table (table 5.1).

The largest group of participants belonged to technology-related fields, followed by business-related disciplines and law. Smaller groups included participants from education, mathematics, and other fields.

This distribution allows the study to include both technical and non-technical perspectives regarding the recognition and interpretation of dark patterns.

Category	Included Responses	Total
Technology	Technology	34
Business / Economics	Business Administration, Business, Marketing, Banking, HR, Hospitality, Auditor, Economics, Business Management, Accountant, Accounting, Shipping	22
Education	Education, Teacher, Preschool Teacher, Kindergarten Teacher, Music Teacher, Education and Psychology, Philology	13
Law	Law	11
Health & Medicine	Medicine, Veterinary Medicine, Biology, Psychology	6
STEM	Mathematics, Mathematics and Statistics, Physics, Architecture	5
Arts & Creative Fields	Graphic Designer, Aesthetician, Journalism, Humanities	7
Public Sector / Other Professions	Civil Servant, Public Employee, Private Sector.	3

Table 5.1: Distribution of Participants by Professional Background

5.2.2 Background Information Results

Figure 5.2 shows how frequently participants use the internet. The results indicate that all participants use the internet very frequently. Specifically, 67% reported using the internet almost constantly throughout the day, while 33% reported using it several times a day. No participants selected lower-frequency options.

This suggests that the sample consists of highly active internet users who regularly interact with online platforms and web interfaces.

How often do you use the internet?

101 απαντήσεις

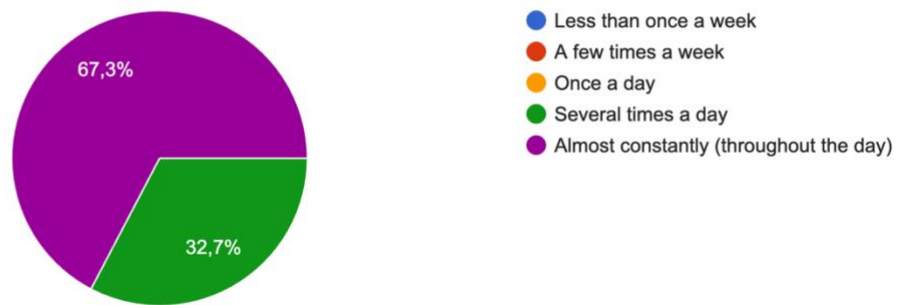


Figure 5.2: How often do you use the internet?

Figure 5.3 presents participants' self-reported familiarity with digital technologies and online privacy. The most common response was 4 (46%), followed by 3(23%) and 5 (19%). Only 12% selected low familiarity levels, with 11% choosing 2 and 1% choosing 1.

Overall, these results show that most participants considered themselves moderately to highly familiar with digital technologies and online privacy.

How would you rate your familiarity with digital technologies or online privacy?

101 απαντήσεις

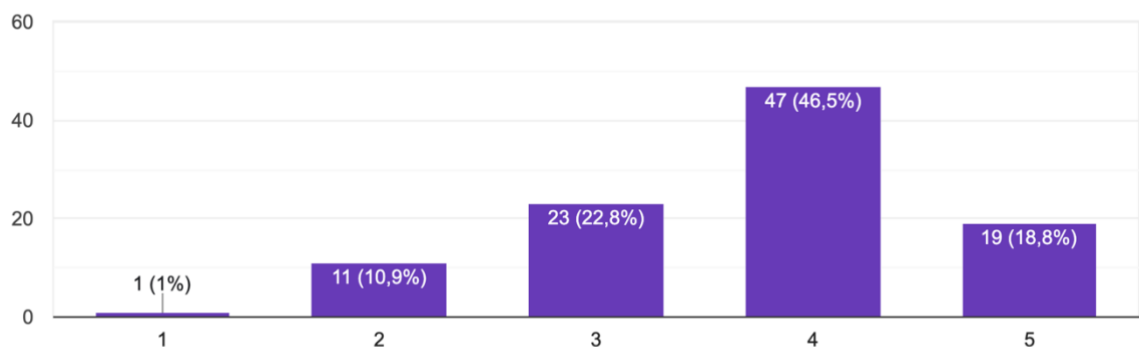


Figure 5.3: How would you rate your familiarity with digital technologies or online privacy?

As shown in Figure 5.4, the majority of participants reported limited prior knowledge of the concept of dark patterns. Specifically, 49% selected the lowest familiarity level, indicating that they had never heard about dark patterns before. In contrast, only 2% reported being completely knowledgeable about the topic.

These results suggest that although participants are highly active internet users, and consider themselves familiar with digital technologies, awareness of the term “dark patterns” and its meaning remains relatively low among them.

Have you heard about dark patterns before?

101 απαντήσεις

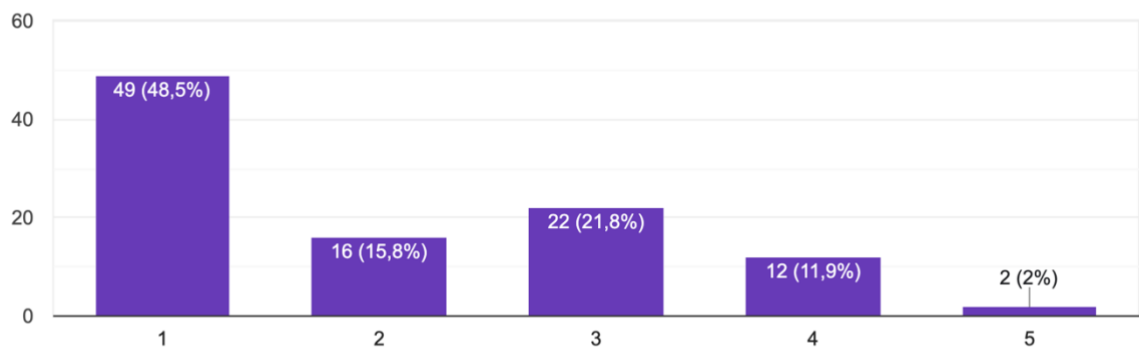


Figure 5.4: Have you heard about dark patterns before?

5.2.3 Dark Patterns on the Web Results

A video was produced for the purposes of this thesis, using the Synthesia.io tool and was embedded in the Google Form questionnaire.

After watching the informational video, participants were asked to respond on how often they believe they are able to recognize and avoid dark patterns while browsing the web.

As shown in Figure 5.5, the majority of responses were concentrated around the middle values of the scale. Specifically, 37.6% of participants selected 3, while 30.7% selected 4. In contrast, only 4% selected the highest value (5), indicating that very few participants felt fully capable of consistently recognizing and avoiding dark patterns.

These results suggest that although many users believe they are sometimes able to identify manipulative interface practices, a significant level of uncertainty still exists when interacting with online environments.

So far, when browsing the web, how often do you think you have been able to recognise and avoid dark patterns?

101 απαντήσεις

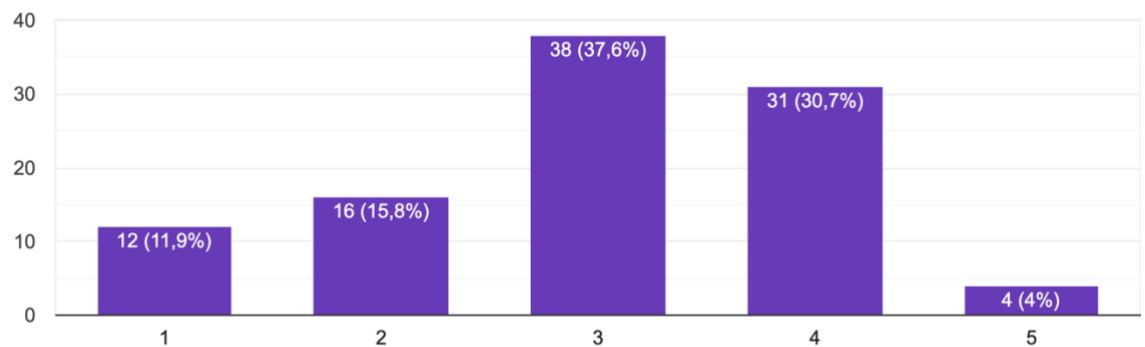


Figure 5.5: So far, when browsing the web, how often do you think you have been able to recognise and avoid dark patterns?

Participants were also asked to rate how confident they feel in recognizing and avoiding dark patterns.

The responses followed a similar distribution pattern. The most common response was again the middle value (3) with 31.7%, followed by 4 (25.7%) and 2 (24.8%). Only 4% of participants selected the highest confidence level.

These findings indicate that while participants may believe they can sometimes identify manipulative practices, they are generally not fully confident in their judgments. This moderate confidence level may reflect the difficulty of distinguishing subtle dark patterns from standard interface design choices.

How confident do you feel in recognising and avoiding dark patterns?

101 απαντήσεις

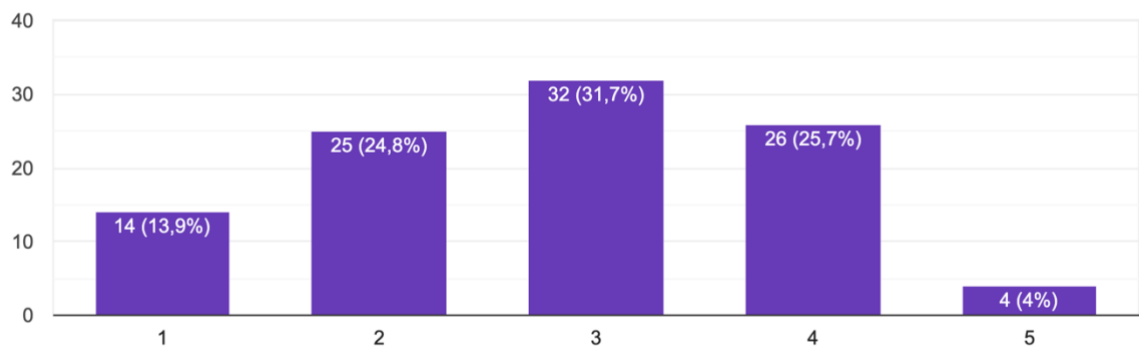


Figure 5.6: How confident do you feel in recognising and avoiding dark patterns?

Participants were finally asked whether they believe that a tool for recognizing and avoiding dark patterns in websites would be useful.

As illustrated in Figure 5.7, the responses were strongly positive. The majority of participants (62.4%) selected the highest value (5), while an additional 24.8% selected 4. No participants selected the lowest value on the scale.

These results indicate a strong interest in supportive mechanisms that help users identify manipulative interface practices. The findings suggest that participants recognize the challenges involved in detecting dark patterns and perceive value in tools designed to improve transparency and user understanding during web interaction.

Do you think a tool for recognising and avoiding dark patterns in websites would be useful?

101 απαντήσεις

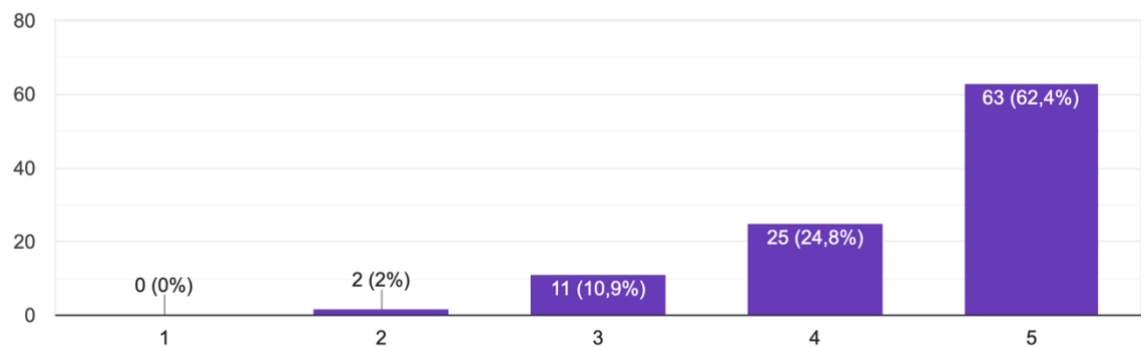
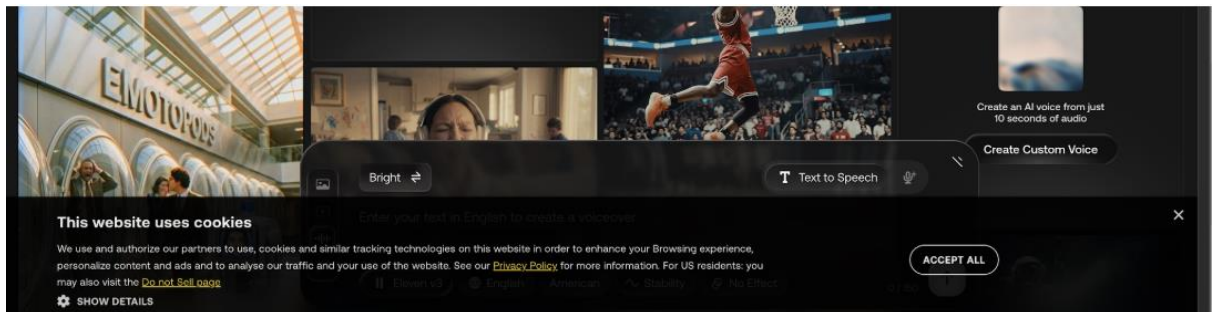


Figure 5.7: Do you think a tool for recognizing and avoiding dark patterns in websites would be useful?

The final part of the questionnaire consisted of the scenario-based evaluation tasks as explained before.

Scenario 1:



The first scenario presented participants with a cookie consent banner containing a manipulative design element - dark pattern “Bad Visibility”. More specifically, the interface prominently displays an “Accept All” option while making the rejection of cookies significantly less visible and less accessible.

As shown in Figure 5.8, participant responses were relatively divided. Specifically, 50,5% of participants answered “Yes,” indicating that they identified the presence of manipulative elements. In contrast, 30,7% answered “No,” while 18.8% selected “I don’t know.”

Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις

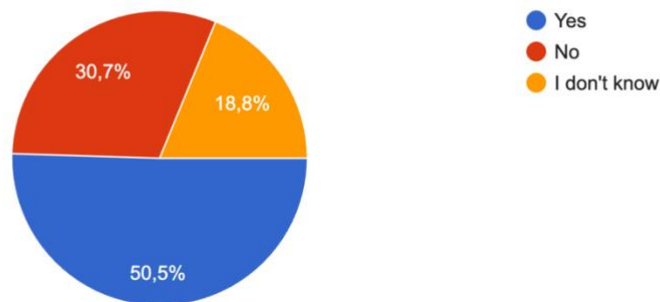


Figure 5.8: Do you think anything in this screen is manipulative or misleading?

These results suggest that although many participants attempted to identify problematic aspects of the interface, recognition of the dark pattern was not consistent across the sample. According to the open-ended questions, some participants successfully identified the absence of a clear rejection option as manipulative (32%), while others either misunderstood the issue (e.g., they recognized that there was an issue in the cookie banner but did not identify the specific manipulative aspect) or failed to recognize the problematic design entirely (e.g., they wrote “N/A” because they did not notice the dark pattern.).

This finding is particularly important because the scenario represented a relatively simple and commonly discussed form of dark pattern. The results therefore indicate that even straightforward manipulative practices may not always be clearly recognized by users during normal web interaction.

Participants were also asked to rate how confident they felt regarding their answers for this scenario.

As shown in Figure 5.9, confidence levels were generally high. The majority of participants selected 4 (34.7%), while 21.8% chose the highest confidence level (5). Only a small percentage reported low confidence levels.

How confident are you in your answer?

101 απαντήσεις

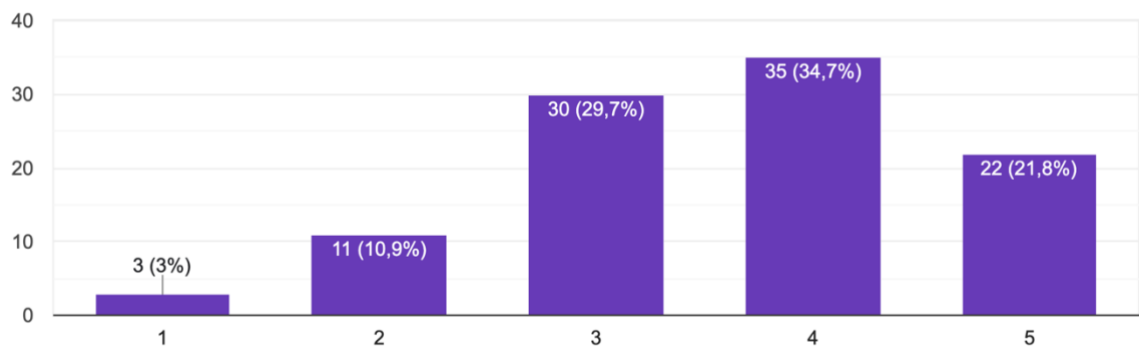


Figure 5.9: How confident are you in your answer?

Scenario 2:

A registration form titled 'Register'. It contains the following fields and elements:

- Email * (text input)
- Username * (text input)
- Password * (password input with a toggle icon)
- Birthdate * (three dropdown menus for Day, Month, and Year)
- ☒ Email me about [redacted] news and events
- ☐ I agree to [redacted] **Terms of Use** and **Privacy Policy ***
- REGISTER button
- Already have an account? [Sign in](#)

The second scenario presented participants with a registration form containing a pre-selected checkbox related to receiving promotional emails and updates. The checkbox was already enabled by default, meaning that users would automatically consent to receiving such communication unless they manually opted out. This is dark pattern “Pressure to receive marketing”

As shown in Figure 5.10, participant responses were again divided. Specifically, 35.6% of participants identified the interface as manipulative, while 48.5% answered “No” and 15.8% selected “I don’t know.”

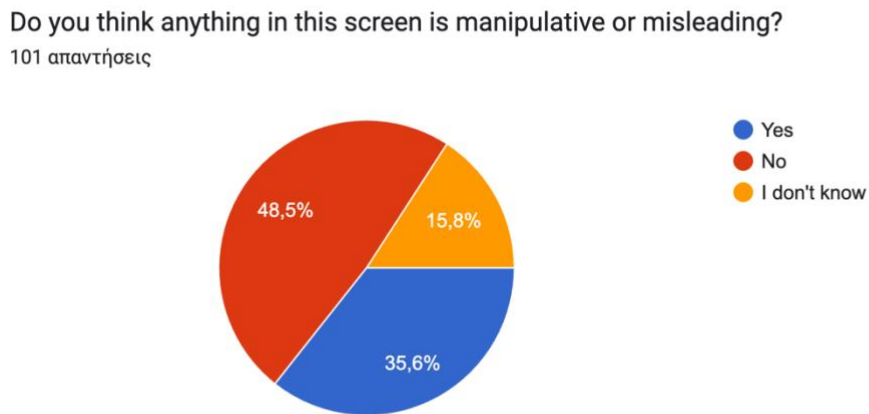


Figure 5.10: Do you think anything in this screen is manipulative or misleading?

The open-ended responses revealed differing interpretations among participants. Several users correctly identified that the checkbox related to promotional emails was already selected by default, with responses such as:

“Email news and events is selected by default”

“The choice of sending me emails for events and news is already chosen”

“The box is already filled”

However, most of the participants stated that they did not notice anything unusual in the interface or considered it a standard registration form. Some responses explicitly mentioned that the interface appeared normal because the information was clearly written.

These findings suggest that pre-selected consent mechanisms may not always be immediately recognized as manipulative

As shown in Figure 5.11, confidence levels were relatively high. The majority of participants selected 4 (34.7%), while 21.8% selected the highest confidence level (5). Only a small percentage selected low confidence values.

How confident are you in your answer?

101 απαντήσεις

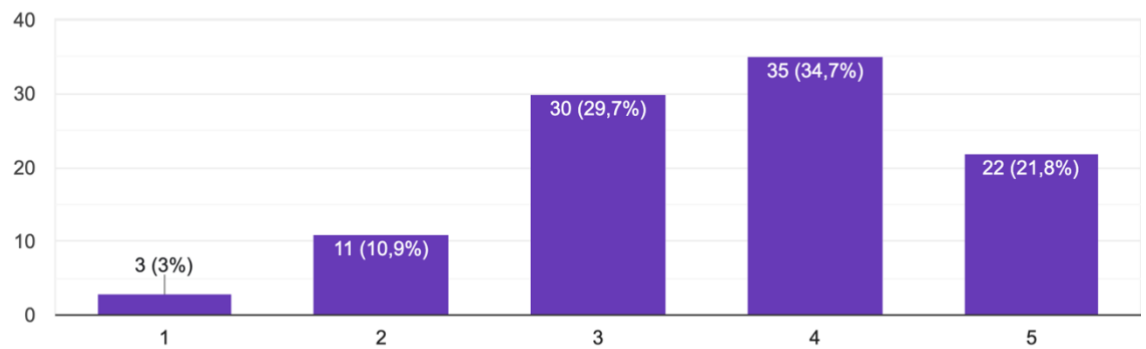
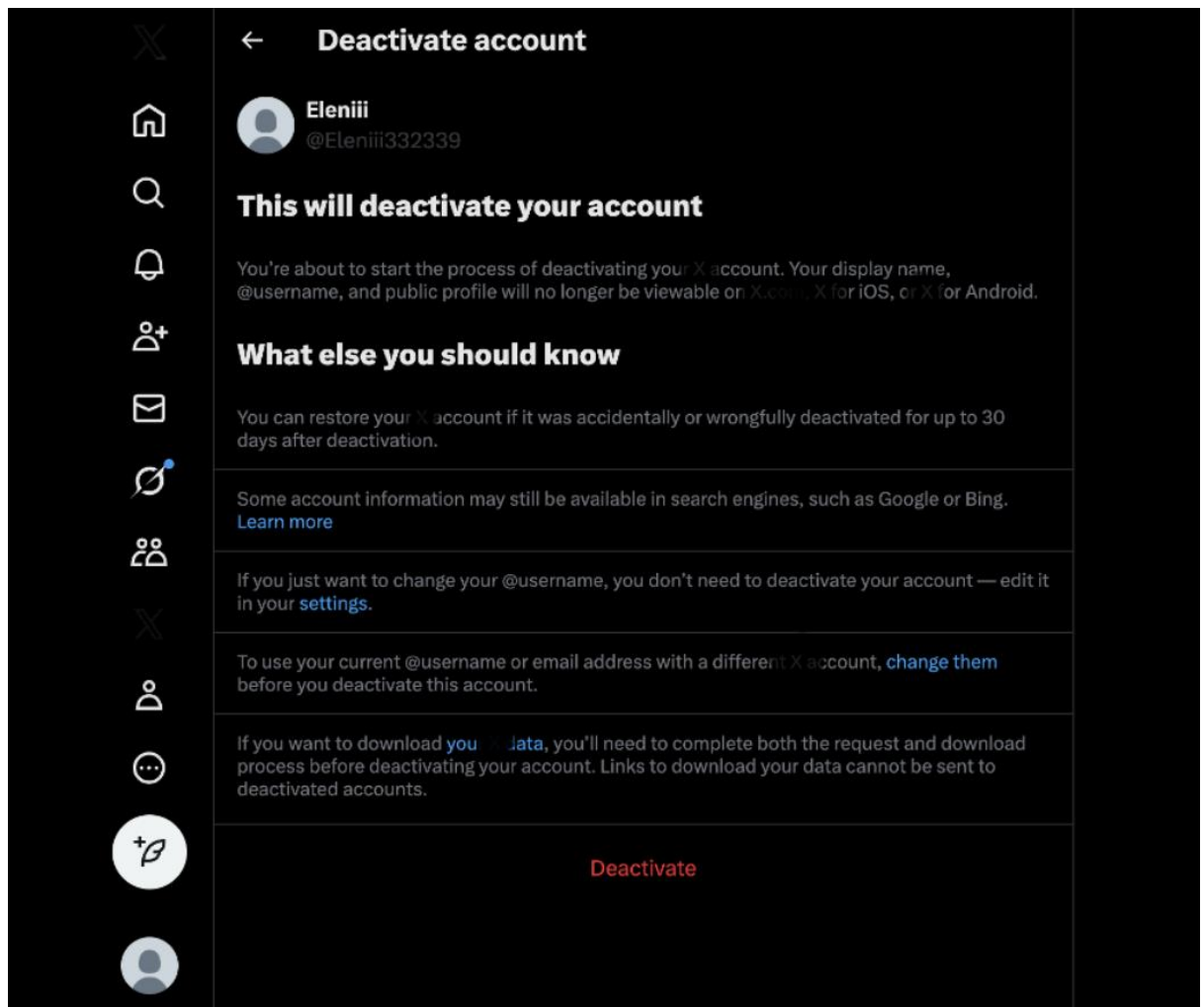


Figure 5.11 How confident are you in your answer?

Scenario 3:



The third scenario presented participants with an account deactivation interface containing multiple warning messages, informational notices, and alternative suggestions before the completion of the process.

As shown in Figure 5.12, the majority of participants did not identify the interface as manipulative. Specifically, 54.5% answered “No,” while only 19.8% answered “Yes.” Additionally, 25.7% selected “I don’t know.”

These findings indicate that most participants interpreted the interface as a normal account management process rather than a potentially manipulative design. Compared to the previous scenarios, recognition of the dark pattern was significantly lower.

One of the main dark pattern elements identified in this interface is that the account is not permanently deleted, but instead temporarily deactivated. Although the interface focuses on the deactivation process, several informational messages indicate that the account may still be recoverable and that some account information may remain accessible.

This may create ambiguity regarding the actual outcome of the process and could potentially mislead users into believing that their account and associated data are completely removed, when in reality the account is only deactivated.

Additionally, the interface contains multiple warning messages and alternative suggestions before the user proceeds with the process. Elements such as repeated notices, references to account recovery, and suggestions to perform alternative actions instead of deactivation may create hesitation and psychological friction during the interaction.

However, most participants did not identify these elements as manipulative or misleading, suggesting that subtle forms of interface ambiguity and discouragement may often go unnoticed during normal web interaction.

These findings indicate that users may struggle to recognize dark patterns when the manipulation relies on psychological discouragement, unclear wording, and indirect interface behavior rather than explicit visual manipulation.

Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις

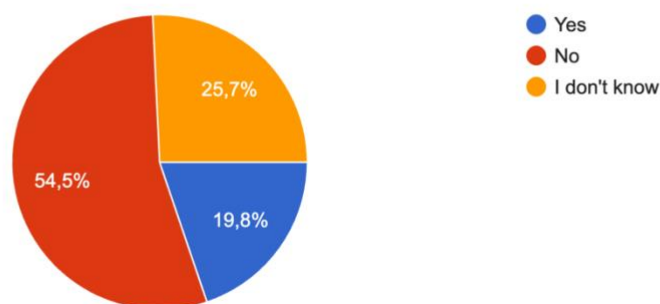


Figure 5.12: Do you think in this screen is manipulative or misleading?

Participants were also asked to rate how confident they felt regarding their answers for this scenario.

As shown in Figure 5.13, the majority of responses were concentrated around moderate confidence levels. Specifically, 34.7% selected 3, while 27.7% selected 4.. Only 11.9% selected the highest confidence value.

How confident are you in your answer?

101 απαντήσεις

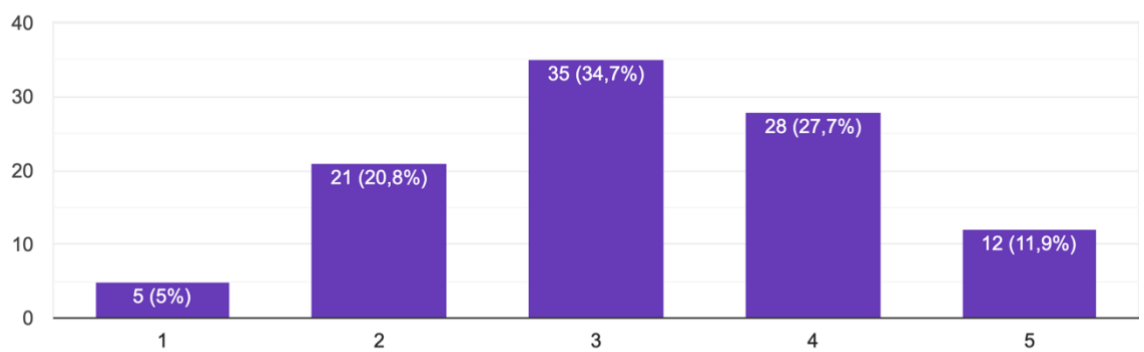


Figure 5.13: How confident are you in your answer?

Scenario 4:

Step 2 of 3

Create a password to start your membership

Just a few more steps and you're done!

We hate paperwork, too.

☐ Please do not email me **Netflix** special offers.

Next

The fourth scenario presented participants with a registration interface containing a checkbox with the statement: “Please do not email me ... special offers.”

The purpose of this scenario was to examine whether participants could recognize a dark pattern based on confusing or misleading wording. Unlike the previous scenarios, the manipulation in this case relied primarily on language structure rather than visual design.

The checkbox uses a double-negative phrasing that may confuse users regarding the actual outcome of their selection. In order to avoid receiving promotional emails, users must carefully interpret the sentence before deciding whether to check or leave the checkbox unchecked.

The participant responses showed that some users successfully identified the manipulative element, while others either misunderstood the interface or were uncertain about the intended meaning of the checkbox. This indicates that language-based dark patterns may still be difficult for many users to recognize during normal interaction with websites.

Additionally, several participants reported confusion regarding whether checking the box would subscribe or unsubscribe them from promotional emails, demonstrating how small wording choices can significantly affect user understanding and decision-making.

As shown in Figure 5.14, the majority of participants did not identify the interface as manipulative or misleading. Specifically, 51.5% answered “No,” while 37.6% answered “Yes.” Additionally, 10.9% selected “I don’t know.”

These findings suggest that although a significant number of participants recognized the manipulative wording, most users still interpreted the interface as normal or acceptable. This indicates that language-based dark patterns may be less noticeable than visually obvious manipulative elements.

Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις

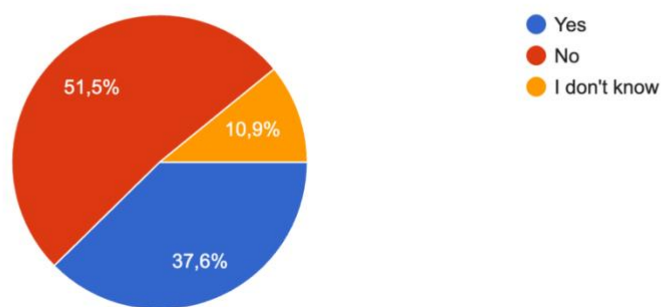


Figure 5.14: Do you think anything in this screen is manipulative or misleading?

As shown in Figure 5.15, confidence levels were generally moderate to high. Specifically, 29.7% selected 3, another 29.7% selected 4, and 25.7% selected the highest confidence value of 5.

How confident are you in your answer?

101 απαντήσεις

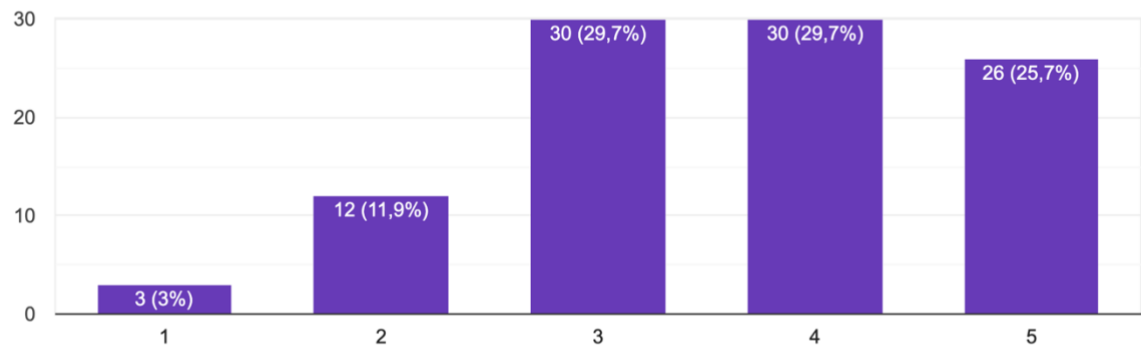


Figure 5.15: How confident are you in your answer?

Scenario 5:

Log in to your account

☐ I am human 
Privacy - Terms

[Reset password](#)

Continue

The fifth scenario presented participants with a standard login interface that did not intentionally contain a dark pattern or manipulative design element.

The purpose of this scenario was to examine whether participants would incorrectly classify a normal interface as manipulative after being exposed to multiple dark pattern examples in the previous scenarios.

As shown in Figure 5.16, the majority of participants correctly identified that the interface was not manipulative or misleading. Specifically, 72.3% answered “No,” while only 8.9% answered “Yes.” Additionally, 18.8% selected “I don’t know.”

These findings suggest that most participants were able to distinguish between manipulative and non-manipulative interfaces when no misleading or obstructive design elements were present.

Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις

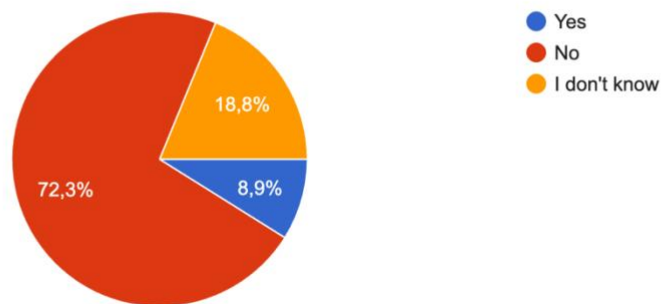


Figure 5.16: Do you think anything in this screen is manipulative or misleading?

Participants were also asked to indicate how confident they felt regarding their answers for this scenario.

As shown in Figure 5.17, confidence levels were generally moderate to high. Specifically, 29.7% selected 3, another 29.7% selected 4, while 23.8% selected the highest confidence value of 5.

These results indicate that most participants felt relatively confident in their judgement when evaluating an interface that did not contain misleading or manipulative elements.

How confident are you in your answer?

101 απαντήσεις

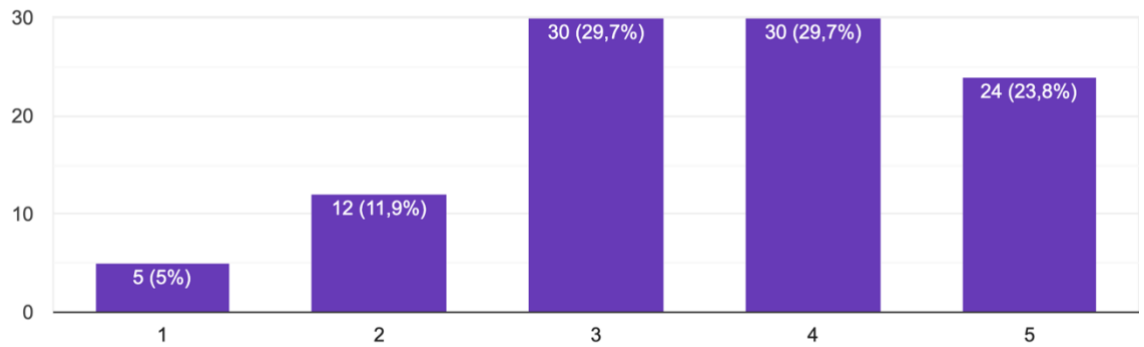


Figure 5.17: How confident are you in your answer?

The following table (table 5.2) presents the survey results for five different scenarios designed to assess participants' ability to recognize and evaluate dark patterns on web interfaces. Each row corresponds to a scenario, and the columns summarize participant responses to the four key questions:

1. Do you think anything on this screen is manipulative or misleading?
->Responses are broken down into Yes, No, and I don't know, showing the percentage of participants selecting each option.
2. If yes, where exactly do you notice it? (% who provided the correct answer)
->Indicates the percentage of participants who correctly identified the location of the manipulative element in the interface.
3. Why do you think it is manipulative, misleading, or unclear? (% who provided the correct answer)
->Shows the percentage of participants who correctly explained the reasoning behind their judgment.
4. How confident are you in your answer?
->Participants rated their confidence on a 1–5 Likert scale, with 1 indicating “Not confident at all” and 5 indicating “Completely confident.”

Scenario	Do you think anything in this screen is manipulative or misleading?			If yes where exactly they notice it? (% who provided the correct answer)	Why do you think it is manipulative, misleading or unclear? (% who provided the correct answer)	How confident are you in your answer?				
	Yes	No	I don't know			1 (Not confident at all)	2	3	4	5 (Completely confident)
Scenario 1	50,5%	30,7%	18,8%	32%	18%	3%	11,9%	30,7%	31,7%	22,8%
Scenario 2	35,6%	48,5%	15,8%	14%	12%	3%	10,9%	29,7%	34,7%	21,8%
Scenario 3	19,8%	54,5%	25,7%	6%	4%	5%	20,8%	34,7%	27,7%	11,9%
Scenario 4	37,6%	51,5%	10,9%	19%	5%	3%	11,9%	29,7%	29,7%	25,7%
Scenario 5	8,9%	72,3%	18,8%	72,3%	72,3%	5%	11,9%	29,7%	29,7%	23,8%

Table 5.2: Scenario-Based Survey Summary

The “I don’t know” column shows participants who were unsure or could not identify any manipulative or misleading parts of the interface. High percentages in this column show where users had trouble spotting dark patterns, even when some participants correctly recognized or explained them. This helps us understand where users find it hard to notice manipulative designs.

5.4 Conclusion

The findings of the questionnaire demonstrate that although participants were highly active internet users and generally familiar with digital technologies, awareness and recognition of dark patterns varied significantly across different types of interface manipulation.

The results indicate that many participants had limited prior knowledge of dark patterns before participating in the study. However, after being introduced to the concept, most participants considered dark patterns to be an important issue and believed that tools

designed to recognise and avoid manipulative interface practices could be useful during online interaction.

An important conclusion of the study is that participants appeared to recognise more obvious and visually explicit manipulative practices more easily than subtle or indirect forms of manipulation. Interfaces relying on confusing wording, psychological discouragement, ambiguity, or increased cognitive effort were often more difficult for participants to identify as manipulative.

The findings also revealed that participants frequently reported moderate or high confidence in their answers, even in cases where manipulative elements were not successfully recognised. This suggests that users may overestimate their ability to identify deceptive or misleading interface practices while browsing the web.

At the same time, the study showed that participants were generally capable of distinguishing between manipulative and non-manipulative interfaces when no deceptive elements were present. This indicates that users are not universally suspicious of online interfaces, but rather face difficulties specifically with subtle forms of manipulation.

Overall, the results of the study highlight the challenges users face in consistently recognising dark patterns during everyday web interaction. The findings support the need for supportive mechanisms and tools that can assist users in identifying such manipulative interface practices more effectively.

In this context, the results strengthen the motivation behind the development of the proposed tool in this thesis. Since many participants struggled to recognise subtle dark patterns or misunderstood manipulative interface elements, a tool capable of analysing and highlighting potentially deceptive practices could help users make more informed decisions while interacting with websites.

Chapter 6

A tool to assist in detecting and mitigating Dark Patterns	70
6.1 Introduction.....	70
6.2 Requirements	71
6.2.1 Functional Requirements	71
6.2.2 Non Functional Requirements	72
6.3 Design.....	73
6.4 Development	74
6.5 Tool Functionalities and Workflow.....	75

6.1 Introduction

In this chapter, a browser-based tool designed and developed to help users detect and understand dark patterns on websites is presented. The chapter is organized as follows: Section 6.1, Requirements, lists both functional and non-functional requirements for the tool. Section 6.2, Design, describes the system architecture and UI prototypes. Section 6.3, Development, covers the technologies and programming languages used, along with an architecture diagram. Finally, Section 6.4, Tool Functionalities, shows screenshots of the tool in action and explains how to use it effectively.

To develop the tool we used an agile software development methodology, as illustrated in Figure 6.1



Figure 6.1 Agile software development technology

6.2 Requirements

6.2.1 Functional Requirements

This subsection presents the requirements of the proposed browser extension/tool, which is designed to assist users in detecting and mitigating dark patterns related to privacy and consent decisions. The functional requirements were derived throughout our research

process from the literature review (Chapter 2), the findings of the manual audit (Chapter 3), and the creation of the taxonomy (Chapter 4).

Additionally, a set of non-functional requirements was added to cover aspects like usability and performance.

Functional Requirements:

ID	Requirement	Description
FR1	Taxonomy Loading	The tool should load and process a structured taxonomy of dark patterns from a JSON file.
FR2	Rule-Based Analysis	The tool should analyze the input using predefined heuristic rules derived from the taxonomy.
FR3	Pattern Detection	The tool should identify potential dark patterns based on matched indicators.
FR4	Pattern Classification	The tool should classify detected cases according to the taxonomy categories.
FR5	Visual Highlighting	The tool should visually highlight suspicious areas within the interface preview.
FR6	Explanatory Feedback	The tool should provide explanations for each detected pattern.
FR7	Result Dashboard	The tool should present a structured dashboard summarizing detected dark patterns.
FR8	Pattern Navigation	The tool should allow users to navigate between detected patterns and corresponding highlighted areas.

6.2.2 Non Functional Requirements

Non Functional Requirements:

ID	Requirement	Description
NFR1	Real-Time Responsiveness	The tool should respond quickly to user input and display results without noticeable delay.
NFR2	Usability	The tool should be easy to use and understandable for non-expert users.
NFR3	Low Intrusiveness	The tool should not overwhelm or confuse users with excessive information or visual clutter.
NFR4	Performance Efficiency	The tool should perform analysis efficiently even with multiple indicators.
NFR5	Extensibility	The tool should support easy addition of new dark patterns and rules.
NFR6	Transparency	The tool should clearly explain why a pattern was detected.
NFR7	Privacy Preservation	The tool should not collect or store unnecessary user data.
NFR8	Maintainability	The system should be modular and easy to update or extend.

6.3 Design

The architecture of the Dark Pattern Detection Tool is modular and fully client-side, meaning all operations run directly in the user's browser without requiring a server.

The tool consists of several interconnected components, each responsible for a specific part of the dark pattern detection process, as presented in Figure 6.2.

This taxonomy component contains the predefined dark patterns (in JSON), their observable indicators, heuristic detection rules, and GDPR mappings. It acts as the core knowledge base of the system and provides the necessary definitions used during the detection process.

To initiate the analysis, the user provides a website URL through the system interface. The submitted webpage is then forwarded to the analysis and detection layer, where the main processing takes place.

The first component of this layer is the Website Analyzer. Through this analysis, the system extracts interface elements and behavioral indicators that may be associated with manipulative design practices.

The extracted information is then processed by the Detection Engine. This component loads the taxonomy definitions and applies heuristic-based rules in order to match the observed webpage indicators with known dark pattern characteristics. The detection engine serves as the core decision-making mechanism of the system.

Following the detection stage, the Dark Pattern Classification module categorizes the identified findings according to the taxonomy structure. In addition, the module generates explanations describing why each pattern was detected and how it relates to manipulative interface behavior.

Finally, the generated results are presented through the Results Dashboard. The dashboard provides a user-friendly visualization of the detected dark patterns, highlights the corresponding webpage elements, and displays contextual explanations for each finding. This allows users to better understand the manipulative techniques identified within the analyzed website.

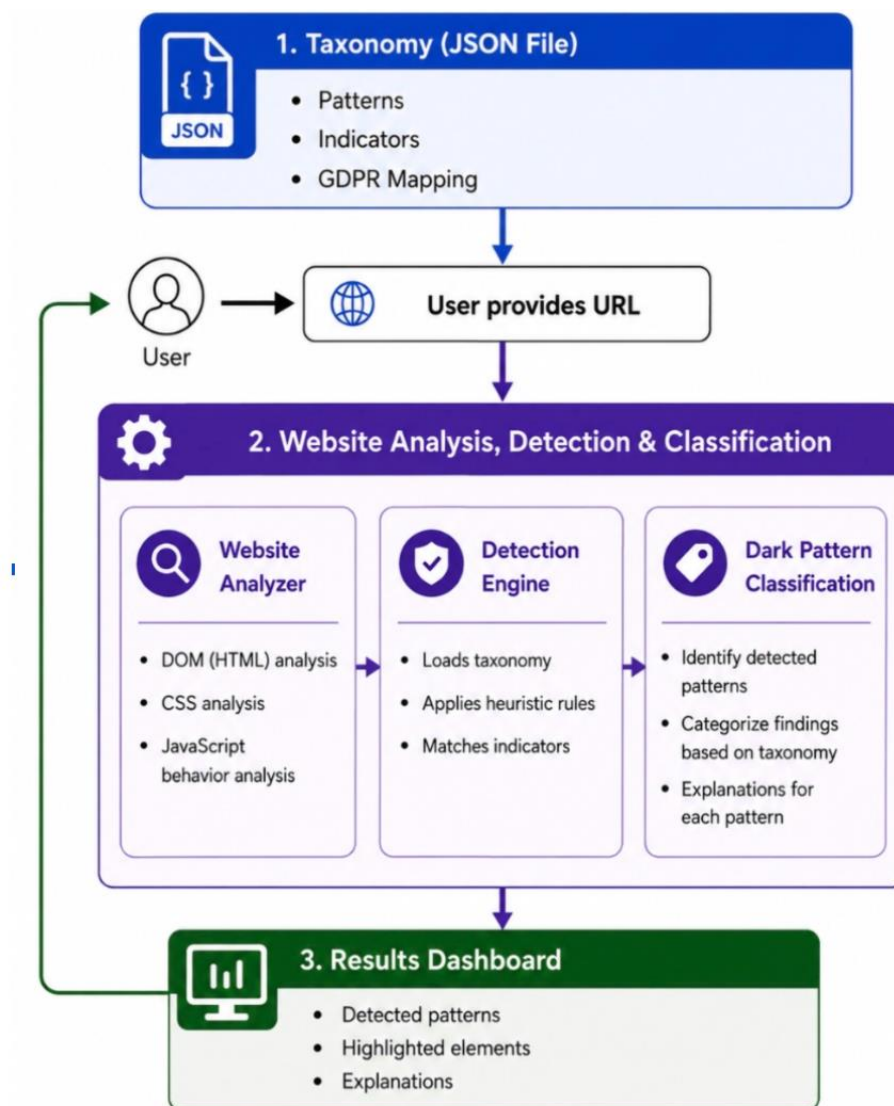


Figure 6.2 System Architecture

6.4 Development

The Dark Pattern Detection Tool was implemented using basic web technologies, ensuring compatibility and ease of deployment. The core technologies employed include

HTML5 for structure, CSS3 for styling and visual highlighting, and JavaScript for dynamic behavior and real-time analysis.

The tool relies on a taxonomy stored as a JSON file, which defines known dark patterns, their indicators, descriptions, GDPR references, prevalence, and associated keywords. These keywords are used during the platform analysis to improve pattern detection and to generate detailed explanations in the results panel and preview highlights.

- **HTML5:** Provides the structure of the interface, including input fields for the website URL, results panels, dashboard sections, and the preview area for detected dark patterns. It ensures that all interactive elements have a consistent layout and are accessible for interaction.
- **CSS3:** Offers styling for the interface, including the visual highlighting of detected dark patterns, labels for the most prominent patterns, and responsive layout adjustments. CSS ensures that highlighted elements and the dashboard are visually distinct, improving user comprehension.
- **JavaScript :** Implements the core functionality of the tool. JavaScript handles user input, triggers analysis, and dynamically updates both the results panel and the website preview. Additionally, it executes the detection logic by collaborating with the taxonomy JSON, applying rule-based heuristics to match inputs and interface elements to known dark patterns. This module ensures real-time detection, classification of patterns, and retrieval of associated details (description, evidence, GDPR references, prevalence, and keywords).
- **JSON Taxonomy:** Contains the structured taxonomy of dark patterns, including pattern descriptions, indicators, GDPR mappings, prevalence statistics, and keywords. These keywords are used to improve detection accuracy, guide the rule-based analysis, and generate detailed explanations in both the results panel and the preview highlighting.

6.5 Tool Functionalities and Workflow

This section provides a step-by-step walkthrough of the Dark Pattern Detection tool's functionality. It provides a visual overview of the tool's operation, showing the process from providing a website URL to the final output of detected dark patterns. Each phase of interaction is accompanied by relevant screenshots.

Step-by-Step Tool Workflow

1. Landing Page & Overview:

The tool provides a web-based interface where users can provide website URLs to identify potential dark patterns.

Instructions and labels guide the user on how to input a URL and interpret results.

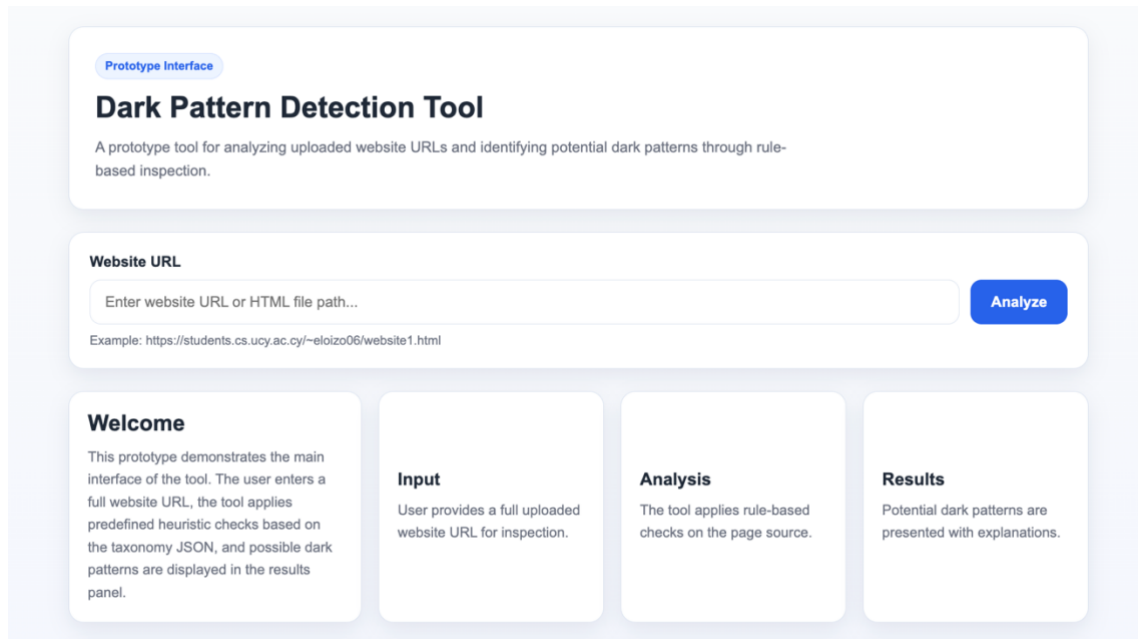


Figure 6.3: Dark Pattern Detection Tool – Landing Page

2. Input Stage:

Website URL field: Users enter the full URL of the website they want to analyze.

This URL serves as the source for the analysis engine.

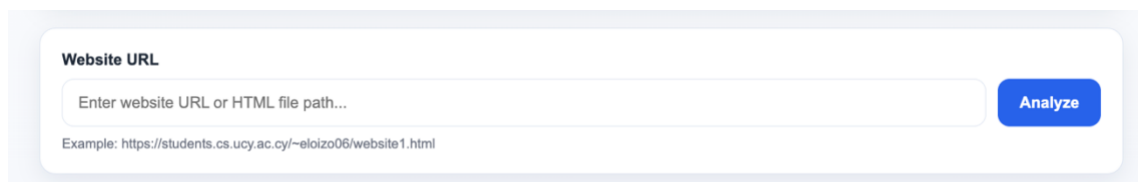


Figure 6.4: Dark Pattern Detection Tool – Input Stage

3. Analysis Engine (in the background):

The tool applies rule-based heuristic checks derived from the JSON taxonomy.

It inspects the page's HTML, CSS, and JavaScript to detect potential dark patterns according to predefined criteria.

4. Results & Findings Panel:

Detected Patterns: Any dark patterns found are displayed in the results panel.

Explanations: Each detected dark pattern is accompanied by an explanation of why it was flagged, helping the user understand the manipulation or misleading element. This includes a description of the pattern, the evidence found on the website, the typical interface location, the corresponding GDPR mapping, and the prevalence in the sample. The data from the taxonomy are exploited.

Initially, before any URL is analyzed, the panel shows “No analysis has been performed yet”.

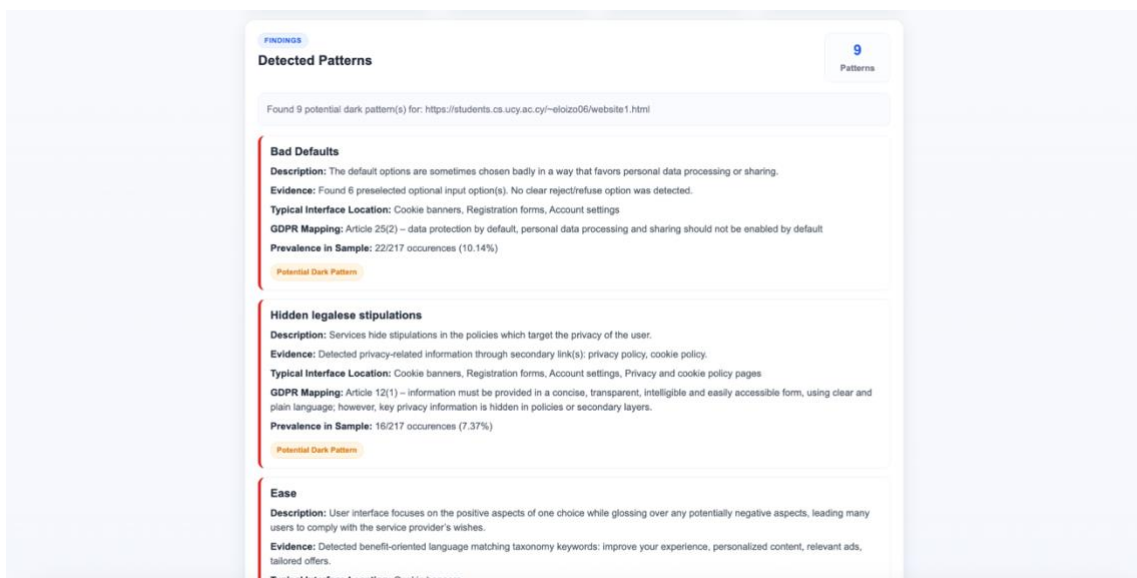


Figure 6.5: Dark Pattern Detection Tool – Results and Findings Panel

5. Output:

Once analysis is complete, the panel updates dynamically with the number of patterns detected and their corresponding details. Users can review each pattern's location and description, providing transparency and actionable insights.

Additionally, the tool includes a live preview of the analyzed website, with the detected dark patterns highlighted directly on the page, allowing users to see exactly where and how manipulative elements appear in context.

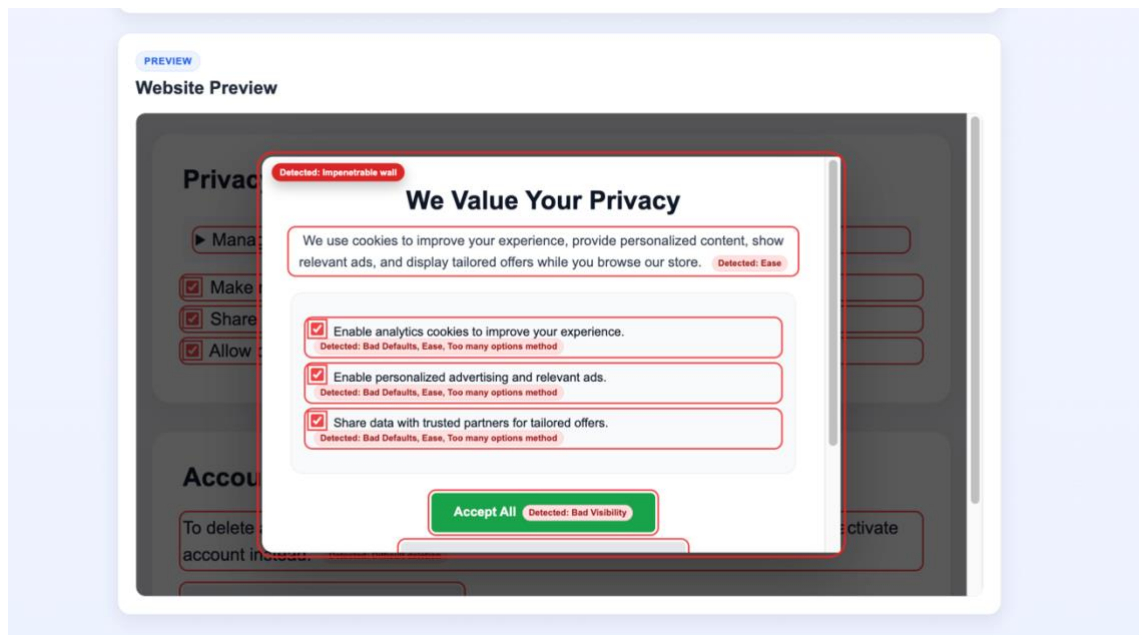


Figure 6.6 Dark Pattern Detection Tool - Output

Chapter 7

Survey called “Dark Patterns Tool Feedback Survey”

Survey called “Dark Patterns Tool Feedback Survey”	79
7.1 Introduction.....	79
7.2 Data Collection	79
7.3 Results	83
7.3.1 Background Information Results	83
7.3.2 User Experience Evaluation Results	86
7.3.3 Usability and Acceptance Results.....	88
7.4 Conclusion	91

7.1 Introduction

Chapter 7 presents the evaluation of the “Dark Patterns Detection Tool”, through a questionnaire-based user study. The purpose of the evaluation was to examine users’ perceptions regarding the usability, understandability, usefulness, and overall effectiveness of the proposed tool in supporting the identification of privacy-related dark patterns on web platforms. The questionnaire was divided into multiple sections, including participants’ background and familiarity with technology and dark patterns, a demo of the tool, user experience evaluation, and usability and acceptance assessment of the tool.

7.2 Data Collection

The evaluation of the proposed “Dark Patterns Detection Tool” was conducted through an anonymous questionnaire-based study using Google Forms. A total of 62 participants took part in the evaluation process. Participation was open and no specific demographic or technical background restrictions were applied, allowing the collection of feedback from users with different levels of familiarity with technology and privacy-related concepts.

The survey consisted of multiple sections.

1) Background Information

The first section collected general background information regarding participants' familiarity with technology and dark patterns. Participants were first asked to indicate their age group by selecting one of the predefined age categories.

The second question asked participants to evaluate their level of familiarity with technology and websites using a five-point Likert scale ranging from "Not familiar at all" (1) to "Fully familiar" (5).

The following question examined how frequently participants use websites or online services in their daily activities. This question also used a five-point Likert scale ranging from "Never" (1) to "Constantly" (5).

Participants were then asked to assess the importance of online privacy using a five-point Likert scale ranging from "Not important at all" (1) to "Extremely important" (5).

Finally, participants evaluated their familiarity with the concept of dark patterns using a five-point Likert scale ranging from "Not familiar at all" (1) to "Fully familiar" (5).

2) Dark patterns Tool - Demo

The second section of the questionnaire introduced participants to the proposed "Dark Patterns Detection Tool". Before proceeding to the evaluation process, participants were asked to watch a short demonstration video presenting the purpose, functionality, and main features of the tool. The video demonstrated how the tool detects and presents privacy-related dark patterns found in web interfaces, allowing participants to better understand the overall operation of the proposed solution.

In addition to the demonstration video, participants were also provided with access to a live online version of the tool through a direct link. This allowed users to interact with the system themselves and explore its functionality in real time before completing the remaining sections of the questionnaire. Participants were encouraged to test the tool using a sample website URL provided within the questionnaire, enabling them to observe how the system analyzes web interfaces and identifies potential dark patterns.

The purpose of this section was to ensure that all participants had sufficient understanding and practical experience with the proposed tool before evaluating its usability, effectiveness, and overall usefulness in the following sections of the survey.

3) User Experience Evaluation

The third section of the questionnaire focused on the User Experience (UX) evaluation of the proposed “Dark Patterns Detection Tool”. This section consisted of 26 evaluation questions based on the User Experience Questionnaire (UEQ)¹ framework, which is widely used for assessing users’ perceptions and overall interaction experience with software systems and digital applications.

4) Usability and Acceptance

The final section of the questionnaire included a set of custom evaluation questions influenced by the Technology Acceptance Model (TAM)² and the System Usability Scale (SUS)³

More specifically, participants were asked:

- Using this tool when using web platforms would increase my privacy awareness and protection.
- I find this tool useful in terms of privacy.
- Using the tool makes me feel confident in detecting and avoiding dark patterns.
- I would use this tool frequently when navigating the web.

¹ <https://www.ueq-online.org/>

² <https://www.academia.edu/>

³ <https://measuringu.com/sus/>

https://youtu.be/pPo_Zxmifl0

All questions in this section were evaluated using a five-point Likert scale ranging from “Completely Disagree” (1) to “Completely Agree” (5).

¹ <https://www.ueq-online.org/>

² <https://www.academia.edu/>

³ <https://measuringu.com/sus/>

https://youtu.be/pPo_Zxmifl0

7.3 Results

7.3.1 Background Information Results

Figure 7.1 presents the age distribution of the participants ($n = 62$). The majority of respondents were young adults aged 18–24, accounting for 75.8% of the sample. Participants aged 25–34 represented 19.4%, while those in the 35–44 age group accounted for 4.8%. No participants were reported in the 45–54, 55–64, or 65+ age groups.

What is your age group?

62 απαντήσεις

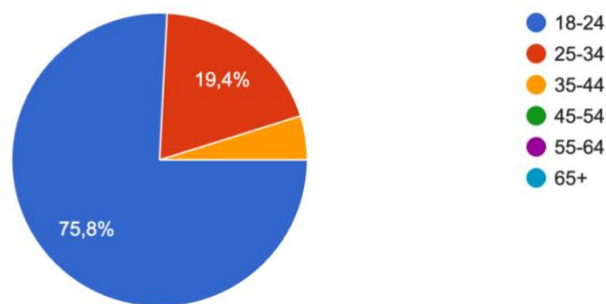


Figure 7.1: What is your age group?

How would you describe your level of familiarity with technology and websites?

62 απαντήσεις

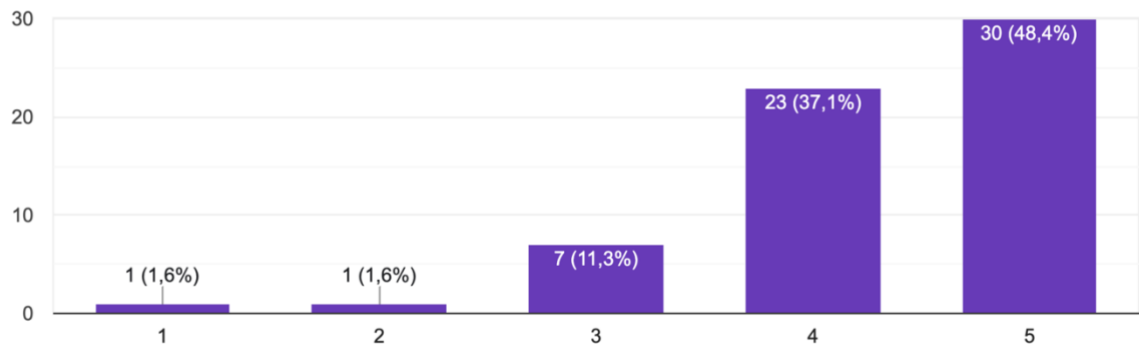


Figure 7.2: How would you describe your level of familiarity with technology and websites?

Figure 7.3 presents participants' frequency of using websites or online services. Responses were collected on a five-point scale, where 1 represents "Never" and 5 represents "Constantly". The distribution of responses are illustrated in the following graph:

How often do you use websites or online services?

62 απαντήσεις

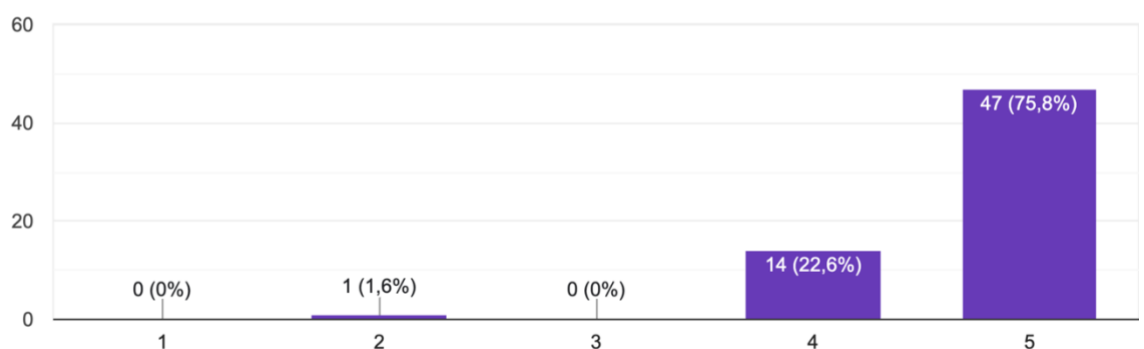


Figure 7.3: How often do you use websites or online services?

The majority of participants reported very frequent use of online services, with 75.8% selecting “Constantly” and 22.6% selecting “4” on the scale. Only a very small fraction of participants (1.6%) indicated low frequency (2 on the scale).

Figure 7.4 presents participants’ responses regarding the importance of online privacy. Participants rated the importance on a five-point scale, where 1 represents “Not important at all” and 5 represents “Extremely important”. The vast majority of participants considered online privacy to be very important, with 71% selecting “Extremely important” and 19.4% selecting “4” on the scale. Only a very small fraction of participants (1.6%) indicated low importance, while none rated it as “Not important at all”.

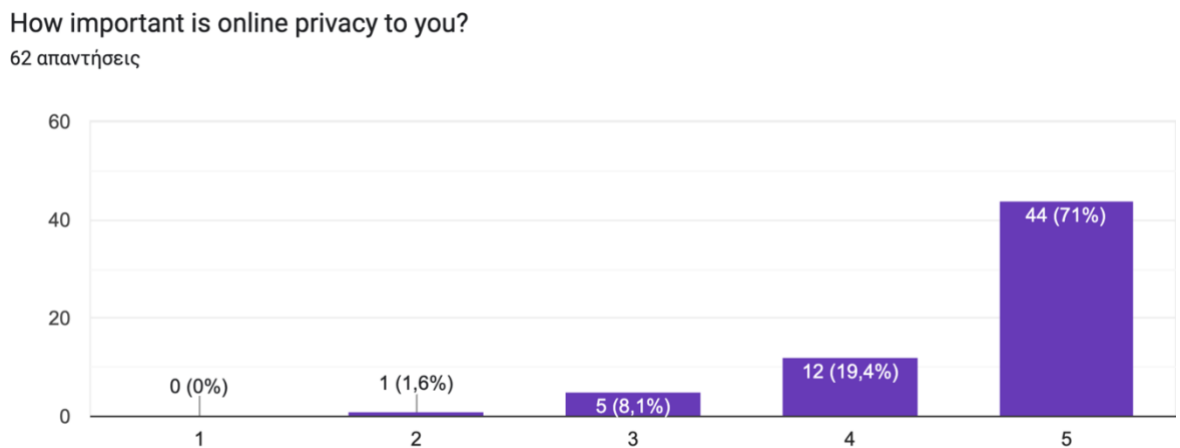


Figure 7.4: How important is online privacy to you?

Figure 7.5 presents participants’ self-reported familiarity with the concept of dark patterns. Participants rated their familiarity on a five-point scale, where 1 represents “Not familiar at all” and 5 represents “Fully familiar”. The results indicate that most participants had only moderate familiarity with dark patterns. While 37.1% selected the middle point (3) on the scale, only a small fraction (4.8%) reported full familiarity. Approximately half of the participants (46.8%) reported low familiarity (1 or 2)

How would you describe your level of familiarity with the concept of 'dark patterns'?

62 απαντήσεις

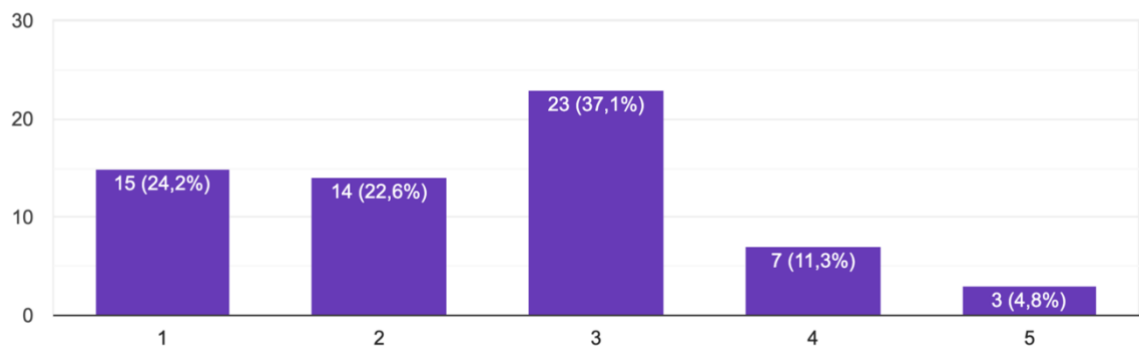


Figure 7.5: How would you describe your level of familiarity with the concept of 'dark patterns'?

7.3.2 User Experience Evaluation Results

This section of the survey examined the perceived user experience of the proposed Dark Patterns Detection Tool using the User Experience Questionnaire (UEQ), consisting of 26 pairs of contrasting attributes rated on a seven-point Likert scale. The UEQ is designed to capture immediate user impressions of a product across six key dimensions: Attractiveness, Perspicuity, Efficiency, Dependability, Stimulation, and Novelty [16]. The mean values for all 26 item pairs are presented in Figure 7.6, transformed onto a scale from -3 (most negative) to +3 (most positive) using the standard UEQ data analysis tool.

Overall, the highest ratings were recorded for not understandable/understandable (2.3), bad/good (2.3), unattractive/attractive (2.3), and unfriendly/friendly (2.3), while the lowest scores were observed for unpredictable/predictable (0.8) and conservative/innovative (1.2). According to the UEQ interpretation guidelines, values above 0.8 represent a positive evaluation; therefore, even the lowest-scoring dimensions indicate a positive user experience.

Moreover, the 26 UEQ items were grouped into the six key dimensions for benchmark-based interpretation (Figure 7.7). Attractiveness (2.2), Perspicuity (2.17), Efficiency

(2.04), Dependability (1.71), and Stimulation (2.13) were rated as Excellent, placing them among the top 10% of benchmarked results. Novelty (1.38) was rated as Good, meaning that approximately 10% of benchmarked products achieved higher scores, while 75% of products scored worse. These results indicate a high-quality user experience across all evaluated dimensions, demonstrating that participants perceived the Dark Patterns Detection Tool as both effective and enjoyable to use.

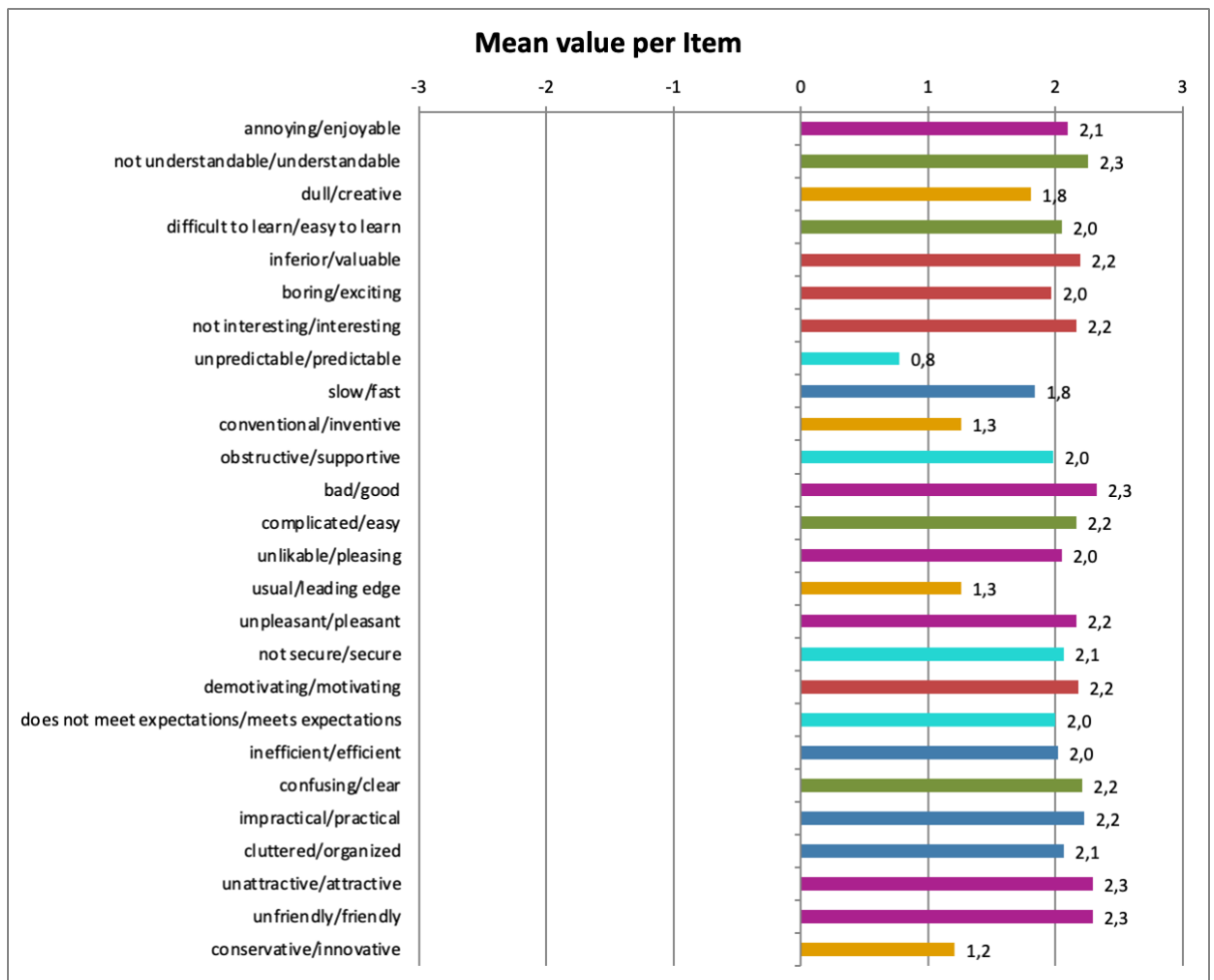


Figure 7.6: Mean value per Item

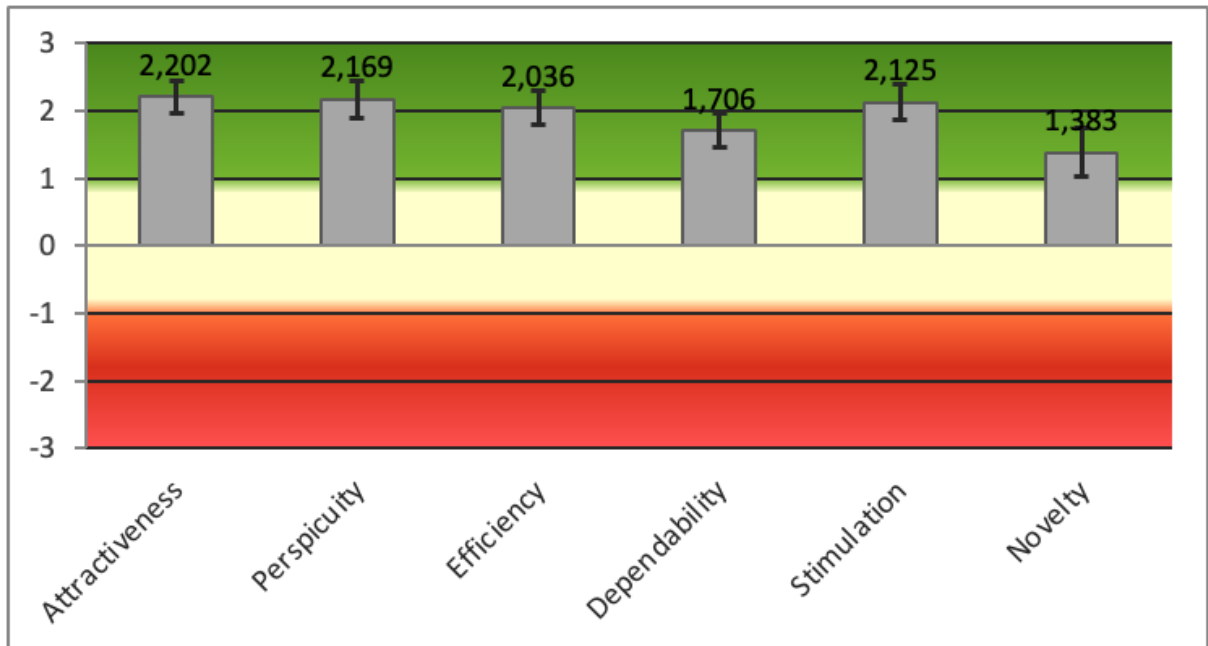


Figure 7.7: UEQ Results: Attractiveness, Perspicuity, Efficiency, Dependability, Stimulation, and Novelty

7.3.3 Usability and Acceptance Results

Figure 7.8 presents participants' responses to the statement "Using this tool when using web platforms would increase my privacy awareness and protection". Participants rated their agreement on a five-point Likert scale, where 1 represents "Completely Disagree" and 5 represents "Completely Agree". The majority of participants (67.7%) strongly agreed that using the Dark Patterns Detection Tool would increase their privacy awareness and protection, while 22.6% agreed moderately. Only a small fraction of participants reported neutral or low agreement (9.7% combined for 1–3 on the scale). This finding indicates that participants perceive the tool as highly effective in enhancing privacy awareness

Using this tool when using web platforms would increase my privacy awareness and protection.
62 απαντήσεις

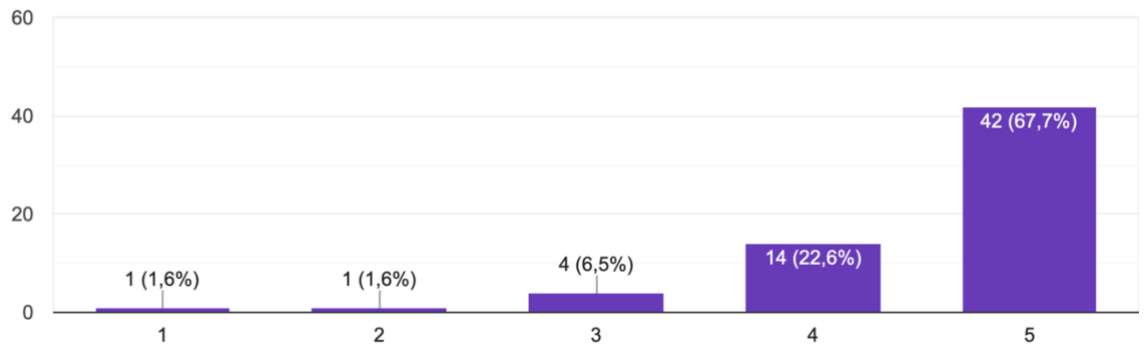


Figure 7.8: Using this tool when using web platforms would increase my privacy awareness and protection

Figure 7.9 presents participants' responses to the statement "I find this tool useful in terms of privacy". Participants rated their agreement on a five-point Likert scale, where 1 represents "Completely Disagree" and 5 represents "Completely Agree". The majority of participants (74.2%) strongly agreed that the Dark Patterns Detection Tool is useful in terms of privacy, while 19.4% selected moderate agreement. Only a small fraction (6.5%) remained neutral.

I find this tool useful in terms of privacy.
62 απαντήσεις

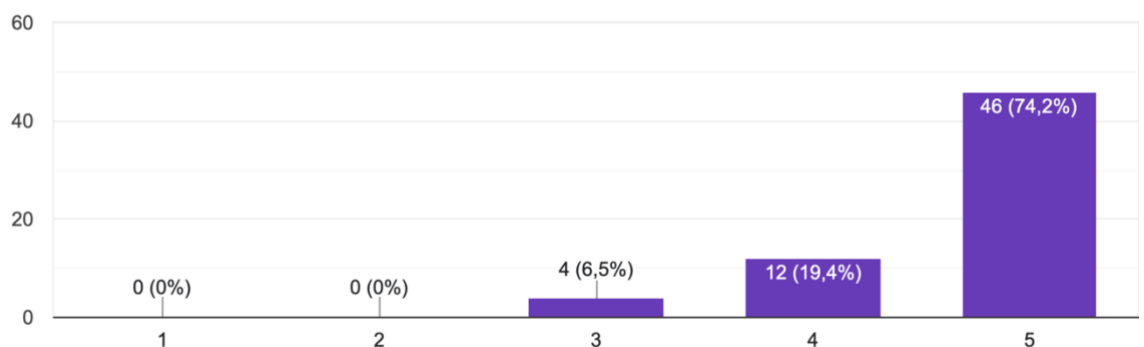


Figure 7.9: I find this tool useful in terms of privacy

Figure 7.10 presents participants' responses to the statement "Using the tool makes me feel confident in detecting and avoiding dark patterns". Participants rated their agreement on a five-point Likert scale, where 1 represents "Completely Disagree" and 5 represents "Completely Agree". The majority of participants (71%) strongly agreed that using the Dark Patterns Detection Tool increased their confidence in detecting and avoiding dark patterns, while 19.4% selected moderate agreement. A smaller fraction of participants (9.7%) remained neutral. This finding indicates that the tool effectively supports users in recognizing manipulative design practices and enhances their confidence in managing online privacy risks.

Using the tool makes me feel confident in detecting and avoiding dark patterns.
62 απαντήσεις

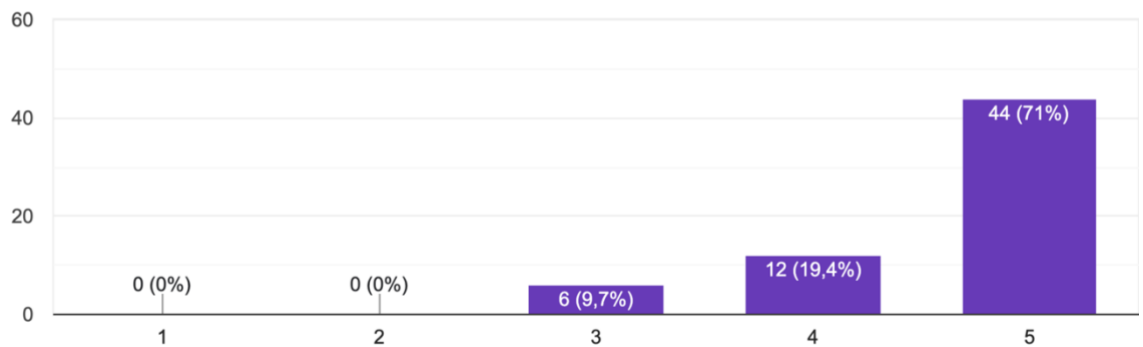


Figure 7.10: Using this tool makes me feel confident in detecting and avoiding dark patterns.

Figure 7.11 presents participants' responses to the statement "I would use this tool frequently when navigating the web". Participants rated their agreement on a five-point Likert scale, where 1 represents "Completely Disagree" and 5 represents "Completely Agree". The majority of participants (58.1%) strongly agreed that they would use the Dark Patterns Detection Tool frequently during their web navigation, while 24.2% expressed moderate agreement. A smaller fraction of participants selected neutral (14.5%) or low agreement (3.2%).

I would use this tool frequently when navigating the web.

62 απαντήσεις

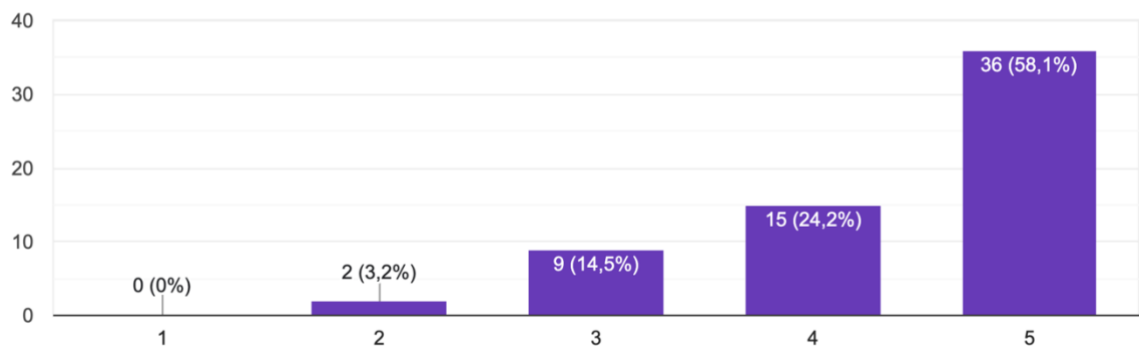


Figure 7.11: I would use this tool frequently when navigating the web.

7.4 Conclusion

The results of the evaluation survey demonstrate that the Dark Patterns Detection Tool is well-received and positively perceived by participants.

Overall, the survey findings confirm that the proposed tool effectively addresses the intended purpose of raising awareness and facilitating the detection of dark patterns, while providing a positive and engaging user experience.

Chapter 8

Conclusion

8.1 Final Remarks	92
8.2 Future Work.....	92

8.1 Final Remarks

This thesis investigated the impact of dark patterns on user interactions with privacy-related interfaces on web applications. Through the development of a structured taxonomy and the implementation of an automated detection tool, the work provided both a conceptual and practical approach to identifying manipulative design strategies that compromise user privacy. The evaluation demonstrated that users often struggle to recognize subtle manipulations in privacy-related interfaces such as consent dialogs, cookie banners, and account settings, highlighting the importance of transparency and clear design principles. The developed tool successfully operationalizes the proposed taxonomy, enabling users to identify and understand manipulative patterns in privacy-related web interfaces. At the same time, the proposed taxonomy and analysis framework provide a structured foundation for developers and researchers to support future studies, improve privacy interface design, and facilitate the development of additional dark pattern detection approaches and tools.

8.2 Future Work

Although this study provides a comprehensive framework and initial evaluation, several avenues remain for future research. First, the taxonomy is designed to be extendable, allowing additional dark patterns to be incorporated as new manipulative strategies emerge. This flexibility ensures that the framework can evolve alongside changes in web interface design and privacy practices. Second, integrating real-time monitoring capabilities for logged-in sessions and dynamic user interactions would allow the tool to detect manipulations beyond static forms. Third, combining automated detection with machine learning approaches could improve pattern recognition, particularly for subtle or evolving manipulative strategies. Finally, further user studies could assess the actual tool's impact on decision-making, usability, and user trust, contributing to a broader understanding of effective privacy-enhancing interventions.

Bibliography

- [1] Vanezi, E., Vasileiou, A., & Papadopoulos, G. A. (2025, September). Making Data Collection Transparent and Usable: Annotating Web Forms with Processing Purposes. In Conference on e-Business, e-Services and e-Society (pp. 288-300). Cham: Springer Nature Switzerland.
- [2] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), Official Journal of the European Union, L119, pp. 1–88, 2016.
- [3] Brignull, H. (2011). Dark patterns: Deception vs. honesty in UI design. *Interaction Design, Usability*, 338, 2-4.
- [4] Jarovsky, L. (2022). Dark patterns in personal data collection: definition, taxonomy, and lawfulness. *Taxonomy, and Lawfulness* (March 1, 2022).
- [5] Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43-109.
- [6] Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., ... & Schaub, F. (2019). An empirical analysis of data deletion and {Opt-Out} choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 387-406).
- [7] Matte, C., Bielova, N., & Santos, C. (2019). Do Cookie Banners Respect my Choice. *Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*. DOI, 10(09).
- [8] Brunotte, W., Chazette, L., Kohler, L., Klunder, J., & Schneider, K. (2022, May). What about my privacy? Helping users understand online privacy policies. In

Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering (pp. 56-65).

- [9] Mathur, A., Kshirsagar, M., & Mayer, J. (2021, May). 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 (pp. 1-18).

- [10] Herbiet, Estelle. Dark Patterns and Privacy Rights in the Digital Age: Evaluating the GDPR and DSA's Regulatory Responses to Deceptive Designs. <https://www.maastrichtuniversity.nl/sites/default/files/2025-06/MWP%202025-4.pdf>

- [11] Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., & de las Heras Ballell, T. R. (2022). Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. Publications Office of the European Union.

- [12] <https://backlinko.com/most-popular-websites>

- [13] https://en.wikipedia.org/wiki/List_of_most-visited_websites

- [14] <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025>

- [15] Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. European journal of information systems, 22(3), 336-359.

- [16] Schrepp, M., Hinderks, A., & Thomaschewski, J. (2017). Construction of a benchmark for the user experience questionnaire (UEQ). *International Journal of Interactive Multimedia and Artificial Intelligence*, 4(4), 40-44.

Appendix A

This appendix presents the full questionnaire used in the study on the effects of dark patterns in consent decisions, as described in Chapter 5. The survey aimed to investigate how users perceive website interfaces and how such designs may influence decisions related to privacy and personal data.

A user study on the effects of dark patterns in consent decisions

* Υποδεικνύει απαιτούμενη ερώτηση

Thank you for participating in this survey, which aims to investigate how users perceive website interfaces and how such designs may influence decisions related to privacy and personal data. *

This research is conducted for academic purposes only, and no monetary benefits are involved. The results will be used in research reports and academic work. Please do not provide any personal or identifiable information. All responses will remain anonymous and will be handled in accordance with data protection regulations.

The survey takes approximately 5–8 minutes to complete and involves answering a series of questions based on your experience and perception.

By completing this survey, you confirm that:

You understand the purpose of the study. Participation is voluntary, and you may withdraw at any time. Your responses will be stored securely and accessed only by the researchers.

By proceeding, you consent to participate voluntarily in this study.

For any questions or concerns, please contact:

Eleni Loizou (University of Cyprus) – eloizo06@ucy.ac.cy

Evangelia Vanezi (University of Cyprus) – vanezievangelia@gmail.com

☐ Yes, I agree

☐ No, I don't agree

Επόμενο

Εκκαθάριση φόρμας

A user study on the effects of dark patterns in consent decisions

* Υποδεικνύει απαιτούμενη ερώτηση

Demographic Information

What is your age group? *

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65+

What is your field of study or work? *

- ☐ Technology
- ☐ Law
- ☐ Άλλο: _____

[Πίσω](#)

[Επόμενο](#)

[Εκκαθάριση φόρμας](#)

Background Information

How often do you use the internet? *

- ☐ Less than once a week
- ☐ A few times a week
- ☐ Once a day
- ☐ Several times a day
- ☐ Almost constantly (throughout the day)

How would you rate your familiarity with digital technologies or online privacy? *

- | | | | | | | |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------------------|
| | 1 | 2 | 3 | 4 | 5 | |
| Not familiar at all | ☐ | ☐ | ☐ | ☐ | ☐ | Completely familiar |

Have you heard about dark patterns before? *

- | | | | | | | |
|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--|
| | 1 | 2 | 3 | 4 | 5 | |
| I have never heard about dark patterns before | ☐ | ☐ | ☐ | ☐ | ☐ | I am completely knowledgeable on dark patterns |

Dark Patterns on the Web

Short Introduction about dark patterns

Dark Patterns
Eleni Loizou

Some options may not clearly show what will happen to your data.

Some options may lead you to share more of your personal data without realizing it.

Help us improve our service

- ☐ Share your email address for updates
- ☒ Share your location for personalized offers

Proceed

Submit

Terms of Service | Privacy Policy | Help Center

Παρακολούθηση σε YouTube

So far, when browsing the web, how often do you think you have been able to recognise and avoid dark patterns? *

	1	2	3	4	5	
Never	☐	☐	☐	☐	☐	Always

How confident do you feel in recognising and avoiding dark patterns? *

	1	2	3	4	5	
Not confident at all	☐	☐	☐	☐	☐	Completely Confident

Do you think a tool for recognising and avoiding dark patterns in websites would be useful? *

	1	2	3	4	5	
Not useful at all	☐	☐	☐	☐	☐	Completely useful

Please carefully inspect the following screen and answer the questions based on your own judgment.



Do you think anything in this screen is manipulative or misleading? *

- ☐ Yes
- ☐ No
- ☐ I don't know

If yes, where exactly do you notice it? If no, please write "N/A". *

Η απάντησή σας

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A". *

Η απάντησή σας

How confident are you in your answer? *

- 1 2 3 4 5
- Not confident at all ☐ ☐ ☐ ☐ ☐ Completely confident

Please carefully inspect the following screen and answer the questions based on your own judgment.

Register

Email *

Username *

Password *



Birthdate *



☒ Email me about Fandom news and events

☐ I agree to Fandom's **Terms of Use** and **Privacy Policy** *

REGISTER

Do you think anything in this screen is manipulative or misleading? *

- ☐ Yes
- ☐ No
- ☐ I don't know

If yes, where exactly do you notice it? If no, please write "N/A". *

Η απάντησή σας

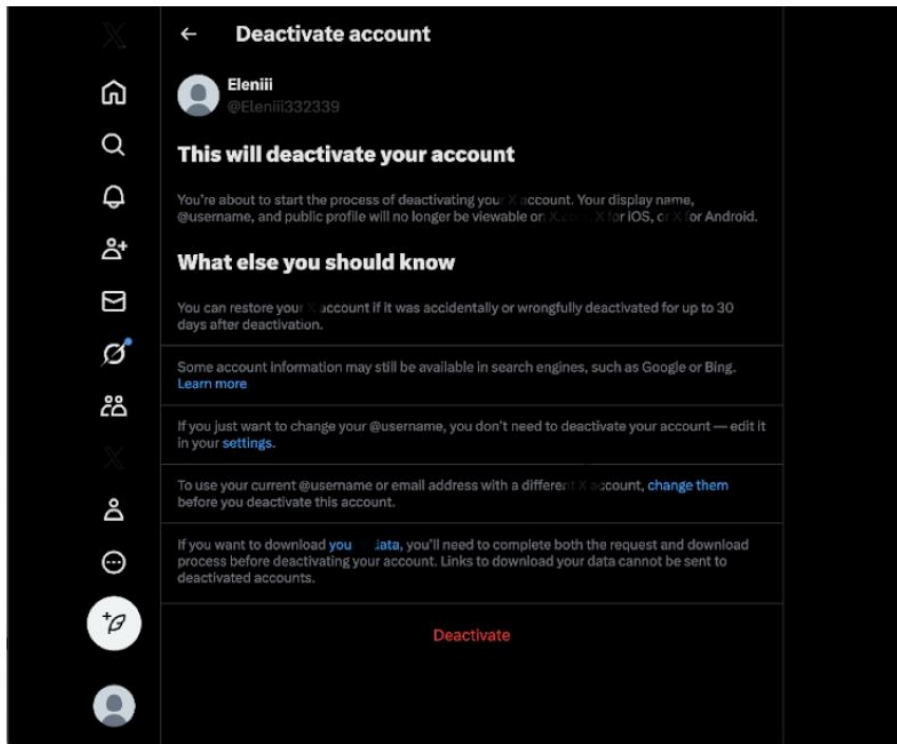
Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A". *

Η απάντησή σας

How confident are you in your answer? *

- | | | | | | | |
|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------------|
| | 1 | 2 | 3 | 4 | 5 | |
| Not confident at all | ☐ | ☐ | ☐ | ☐ | ☐ | Completely confident |

Please carefully inspect the following screen and answer the questions based on your own judgment.



Do you think anything in this screen is manipulative or misleading? *

- ☐ Yes
- ☐ No
- ☐ I don't know

If yes, where exactly do you notice it? If no, please write "N/A". *

Η απάντησή σας

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A". *

Η απάντησή σας

How confident are you in your answer? *

	1	2	3	4	5	
Not confident at all	☐	☐	☐	☐	☐	Completely confident

Please carefully inspect the following screen and answer the questions based on your own judgment.

Step 2 of 3

Create a password to start your membership

Just a few more steps and you're done!

We hate paperwork, too.

☐ Please do not email me **Netflix** special offers.

Next

Do you think anything in this screen is manipulative or misleading? *

- ☐ Yes
- ☐ No
- ☐ I don't know

Do you think anything in this screen is manipulative or misleading? *

- ☐ Yes
- ☐ No
- ☐ I don't know

If yes, where exactly do you notice it? If no, please write "N/A". *

Η απάντησή σας

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A". *

Η απάντησή σας

How confident are you in your answer? *

- | | | | | | | |
|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------------|
| | 1 | 2 | 3 | 4 | 5 | |
| Not confident at all | ☐ | ☐ | ☐ | ☐ | ☐ | Completely confident |

Please carefully inspect the following screen and answer the questions based on your own judgment.



Log in to your British Airways account



I am human



hCaptcha
Privacy - Terms

[Reset password](#)

Continue

Do you think anything in this screen is manipulative or misleading? *

- ☐ Yes
- ☐ No
- ☐ I don't know

If yes, where exactly do you notice it? If no, please write "N/A" *

Η απάντησή σας

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A". *

Η απάντησή σας

How confident are you in your answer? *

- | | | | | | | |
|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------------|
| | 1 | 2 | 3 | 4 | 5 | |
| Not confident at all | ☐ | ☐ | ☐ | ☐ | ☐ | Completely confident |

Appendix B

This appendix presents the full results of the questionnaire used in the study on the effects of dark patterns in consent decisions, as described in Chapter 5. The survey aimed to investigate how users perceive website interfaces and how such designs may influence decisions related to privacy and personal data.

Thank you for participating in this survey, which aims to investigate how users perceive website interfaces and how such designs may influence decisions related to privacy and personal data. *

This research is conducted for academic purposes only, and no monetary benefits are involved. The results will be used in research reports and academic work. Please do not provide any personal or identifiable information. All responses will remain anonymous and will be handled in accordance with data protection regulations.

The survey takes approximately 5–8 minutes to complete and involves answering a series of questions based on your experience and perception.

By completing this survey, you confirm that:

You understand the purpose of the study. Participation is voluntary, and you may withdraw at any time. Your responses will be stored securely and accessed only by the researchers.

By proceeding, you consent to participate voluntarily in this study.

For any questions or concerns, please contact:

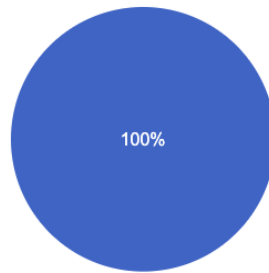
Eleni Loizou (University of Cyprus) – eloizo06@ucy.ac.cy

Evangelia Vanezi (University of Cyprus) – vanezievangelia@gmail.com

☐ Yes, I agree

☐ No, I don't agree

101 απαντήσεις



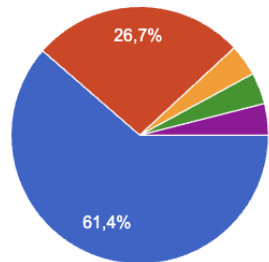
- Yes, I agree
- No, I don't agree

Demographic Information

What is your age group?

101 απαντήσεις

Αντιγραφή γραφήματος

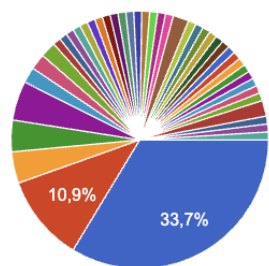


- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

What is your field of study or work?

101 απαντήσεις

Αντιγραφή γραφήματος



- Technology
- Law
- Business Administration
- Education
- Accounting
- Mathematics
- Teacher
- Business

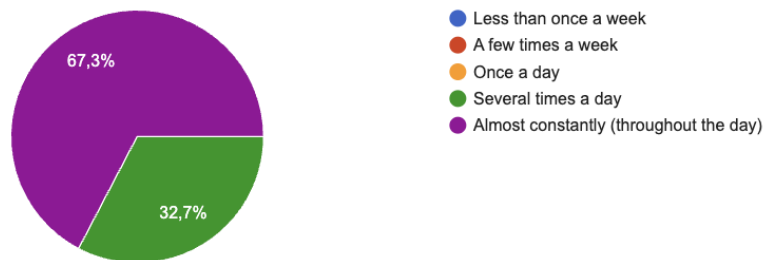
▲ 1/6 ▼

Background Information

How often do you use the internet?

101 απαντήσεις

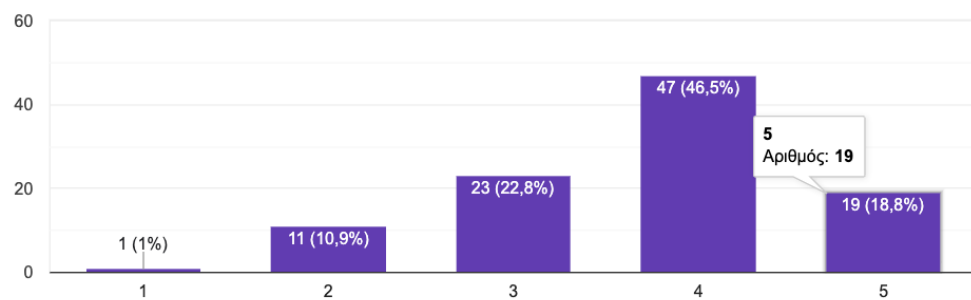
Αντιγραφή γραφήματος



How would you rate your familiarity with digital technologies or online privacy?

101 απαντήσεις

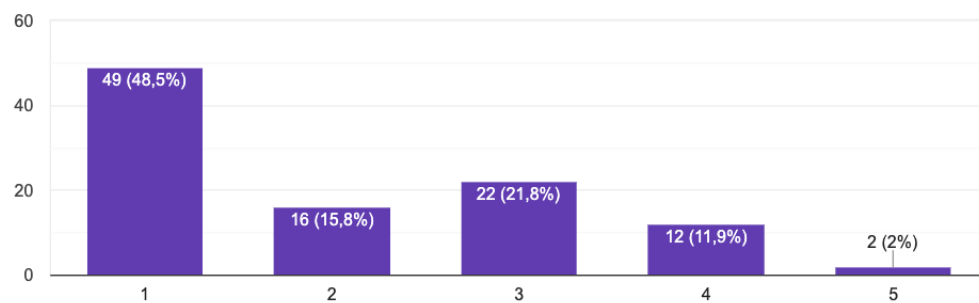
Αντιγραφή γραφήματος



Have you heard about dark patterns before?

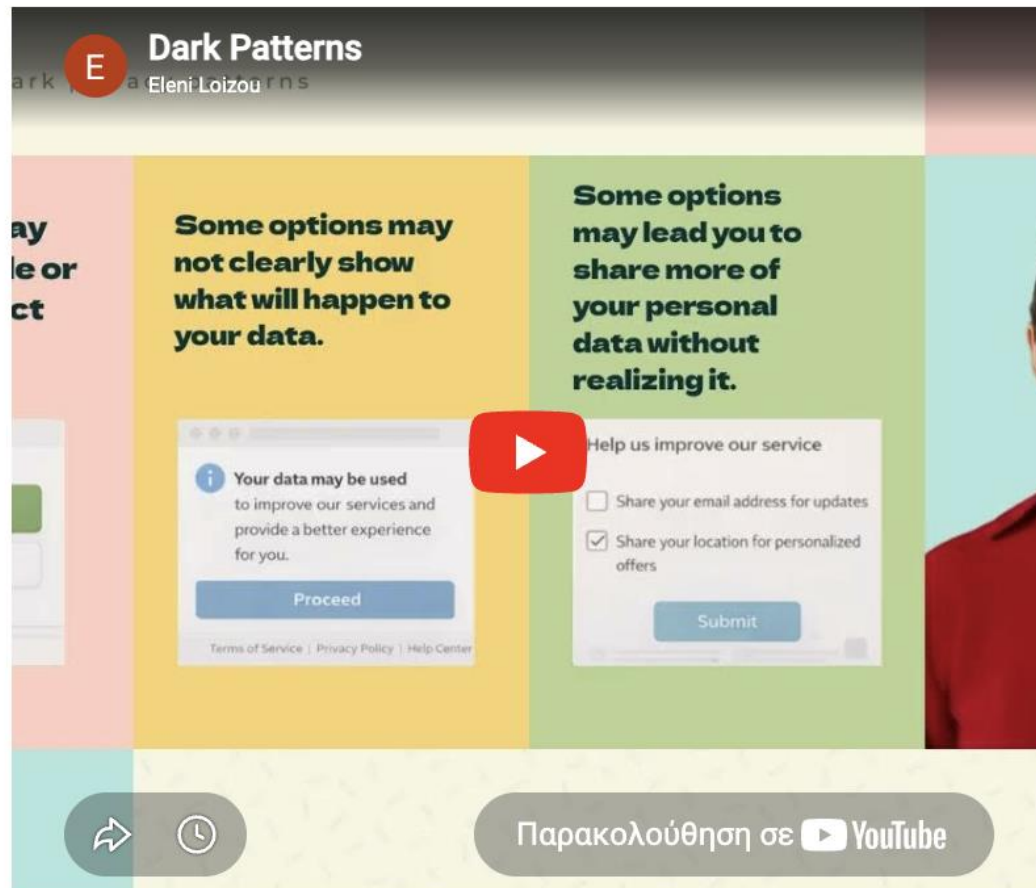
101 απαντήσεις

Αντιγραφή γραφήματος



Dark Patterns on the Web

Short Introduction about dark patterns

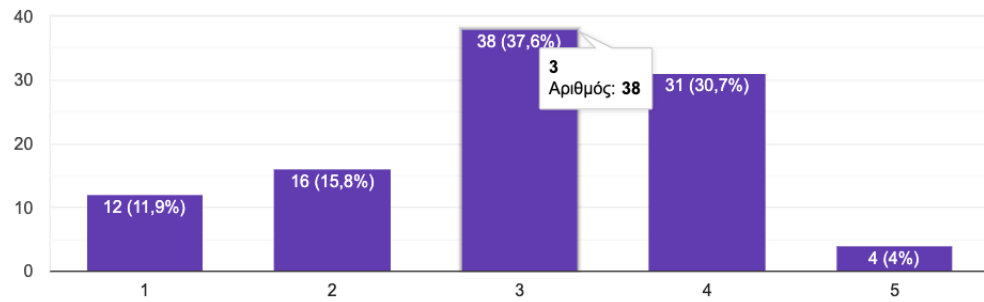


Dark Patterns on the Web

So far, when browsing the web, how often do you think you have been able to recognise and avoid dark patterns?

 Αντιγραφή γραφήματος

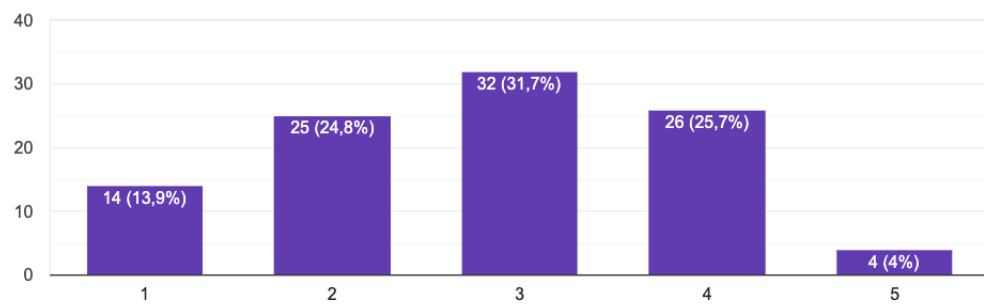
101 απαντήσεις



How confident do you feel in recognising and avoiding dark patterns?

 Αντιγραφή γραφήματος

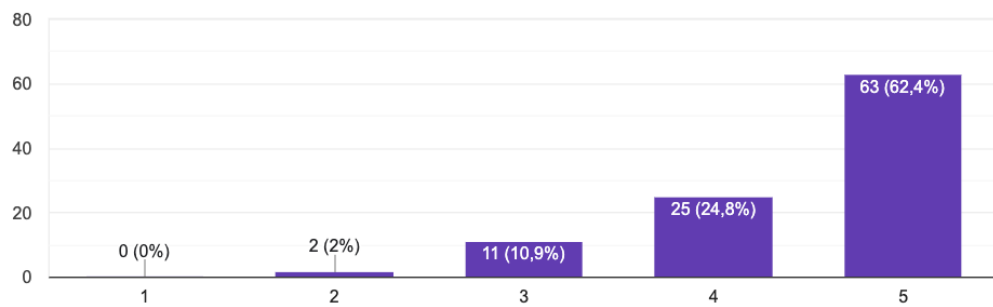
101 απαντήσεις



Do you think a tool for recognising and avoiding dark patterns in websites would be useful?

 Αντιγραφή γραφήματος

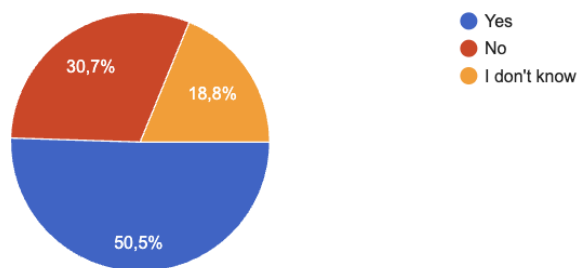
101 απαντήσεις



Do you think anything in this screen is manipulative or misleading?

 Αντιγραφή γραφήματος

101 απαντήσεις



If yes, where exactly do you notice it? If no, please write "N/A".

101 απαντήσεις

N/A

NA

na

Accept the cookies

At the bottom right - Accept All

Only accept all option

Only option is Accept All, doesn't have option to decline

Na

Cookies

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A".

101 απαντήσεις

N/A

NA

Na

N/a

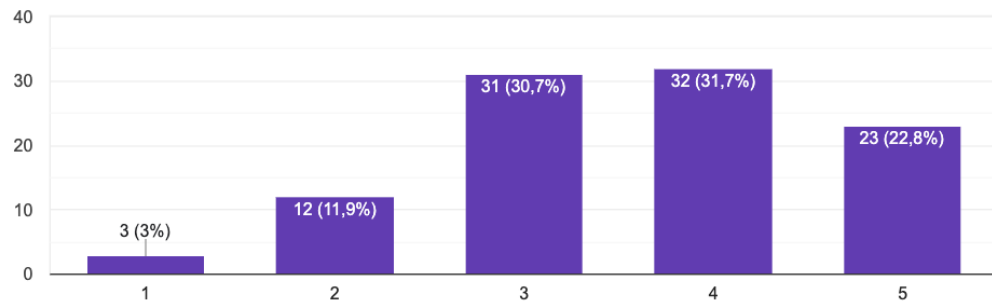
No other option is visible

Reject all should be available too

NA

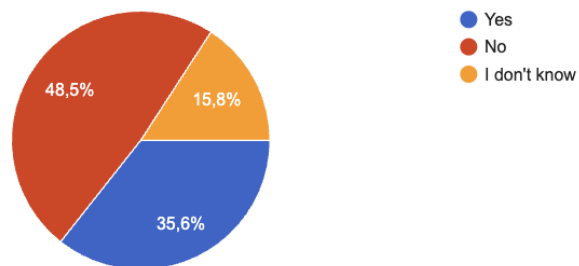
How confident are you in your answer?

101 απαντήσεις



Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις



If yes, where exactly do you notice it? If no, please write "N/A".

101 απαντήσεις

N/A

NA

Na

n/a

Email me about....

Email news and events is selected by default

The choice of sending me emails for events and news is already chosen

I don't find anything unusual, since everything is written correctly, etc. I don't see anything that suggests it is a dark pattern.

the box is already filled

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A".

101 απαντήσεις

N/A

NA

Na

n/a

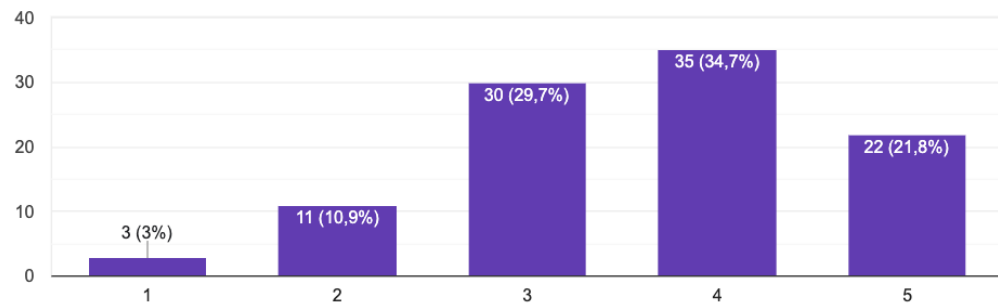
Because is already ticked

Might not be noticed by user

Because I may not want to receive emails about those news and events. It's my choice to make not the

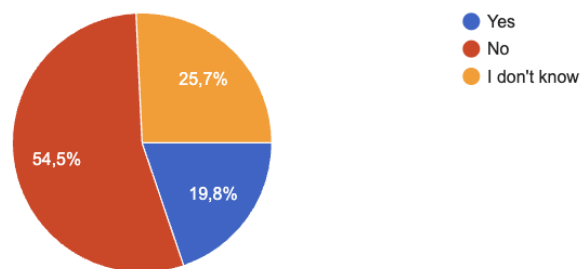
How confident are you in your answer?

101 απαντήσεις



Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις



If yes, where exactly do you notice it? If no, please write "N/A".

101 απαντήσεις

In the info provided.

Some account information may still be available...

Maybe the blue words

when seeing the email user

The "Deactivate" button is visually emphasized in red at the bottom, while alternative options (like editing username or downloading data) are less prominent and embedded in text.

"Some account information may still be available.."

kk

some accounts...or bing

The info about the data of the account after the deactivation

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A".

101 απαντήσεις

N/A

NA

N/a

n/a

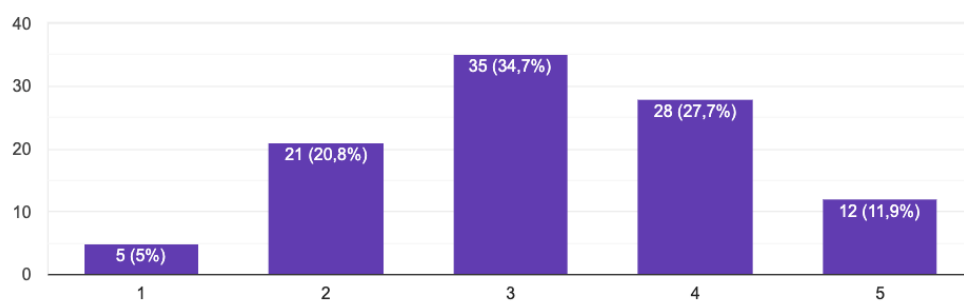
Na

na

It's ill-intentioned as it is likely intended to overload the user with confusing, unrelated information to

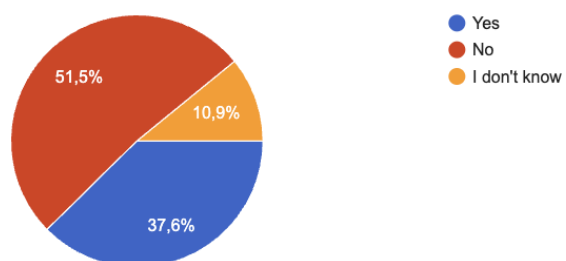
How confident are you in your answer?

101 απαντήσεις



Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις



If yes, where exactly do you notice it? If no, please write "N/A".

101 απαντήσεις

Please do not email me

Please do not email me ...

Check box for emailing special offers

It does not have a privacy policy to agree to

Show password is missing

The instruction above the word "Next"

N/Q

at the checkbox

It requires the user to explicitly request not to receive promotional emails.

We hate paperwork, too

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A".

101 απαντήσεις

N/A

NA

Na

na

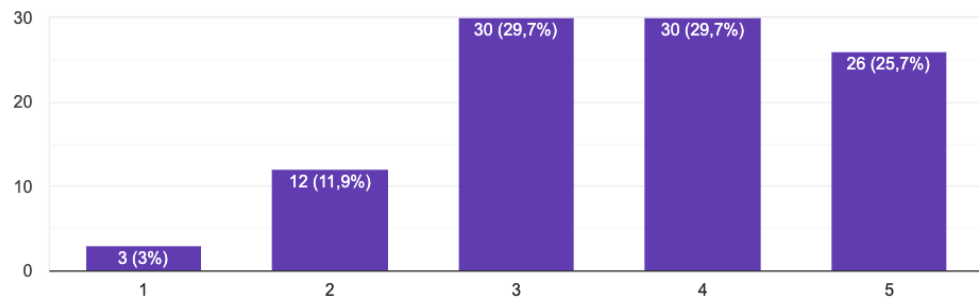
N/a

Because it says please do not email me instead of please email me ... special offers

Because it says 'do not email me' and user needs to check the box

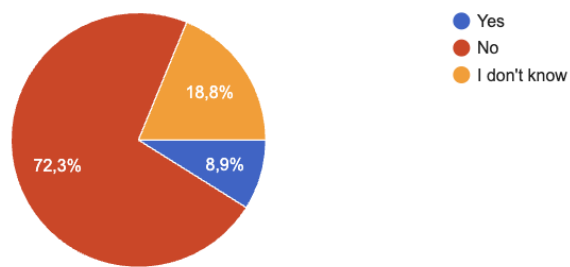
How confident are you in your answer?

101 απαντήσεις



Do you think anything in this screen is manipulative or misleading?

101 απαντήσεις



If yes, where exactly do you notice it? If no, please write "N/A"

97 απαντήσεις

N/A

NA

N/a

n/a

I am human

Na

i am human

Am a human

membership number

Why do you think it is manipulative, misleading, or unclear? If not applicable, please write "N/A".

98 απαντήσεις

N/A

NA

N/a

n/a

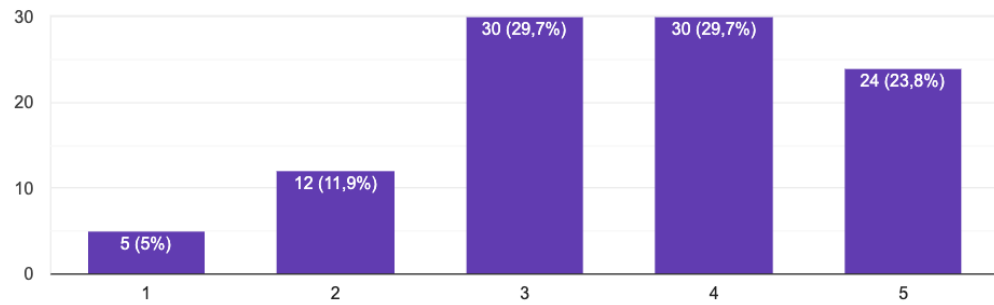
Na

N/A

The robot is asking the human if its human

How confident are you in your answer?

101 απαντήσεις



Appendix C

This appendix includes the full questionnaire used in Chapter 07 to evaluate the Dark Patterns Detection Tool's usability, visual appeal, and effectiveness. The survey was distributed to users as part of the final evaluation phase, aiming to collect feedback on their overall experience with the tool.

*

Thank you for participating in this survey, which aims to evaluate the usability, clarity, and overall user experience of a tool designed to detect dark patterns in websites.

This research is non-commercial, and researchers receive no monetary benefits. Your responses are anonymous and will be used strictly for research purposes, including academic reports and publications. Please do not provide any personally identifiable information.

The survey takes approximately **5-10 minutes** and involves interacting with the tool and answering a short set of questions.

By completing this survey, you confirm that:

You understand the survey's purpose.

Participation is voluntary and you can withdraw at any time.

Your responses will be securely stored and only accessed by the research team.

For any questions or concerns, please contact:

Eleni Loizou (University of Cyprus) – eloizo06@ucy.ac.cy

Evangelia Vanezi (University of Cyprus) – vanezievangelia@gmail.com

☐ Yes, I agree

☐ No, I don't agree

Background Information

What is your age group? *

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65+

How would you describe your level of familiarity with technology and websites? *

- | | 1 | 2 | 3 | 4 | 5 | |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------|
| Not familiar at all | ☐ | ☐ | ☐ | ☐ | ☐ | Fully familiar |

How often do you use websites or online services? *

- | | 1 | 2 | 3 | 4 | 5 | |
|-------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|------------|
| Never | ☐ | ☐ | ☐ | ☐ | ☐ | Constantly |

How important is online privacy to you? *

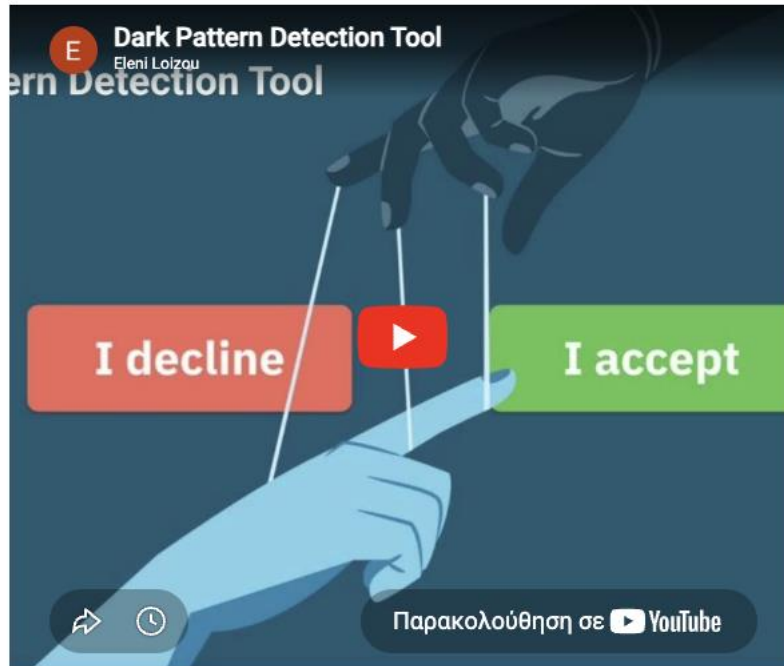
- | | 1 | 2 | 3 | 4 | 5 | |
|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------------------|
| Not important at all | ☐ | ☐ | ☐ | ☐ | ☐ | Extremely important |

How would you describe your level of familiarity with the concept of 'dark patterns'? *

- | | 1 | 2 | 3 | 4 | 5 | |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------|
| Not familiar at all | ☐ | ☐ | ☐ | ☐ | ☐ | Fully familiar |

Dark Patterns Tool - Demo

Before you continue, please watch this demo to understand the purpose and functionality of the Dark Patterns Detection Tool. This will help you provide more accurate feedback.



You may also access and interact with the tool live using the following link: <https://students.cs.ucy.ac.cy/~eloizo06/index.html>.

To test the tool, you may use the following example website URL as input:
<https://students.cs.ucy.ac.cy/~eloizo06/website1.html>

User Experience Evaluation

For the assessment of the tool, please fill out the following questionnaire.
The questionnaire consists of pairs of contrasting attributes that may apply to the tool.

Please remember: there is no wrong or right answer!

Please assess the tool now by ticking one circle per line.

*

	1	2	3	4	5	6	7	
Annoying	☐	☐	☐	☐	☐	☐	☐	Enjoyable

*

	1	2	3	4	5	6	7	
Not understandable	☐	☐	☐	☐	☐	☐	☐	Understandable

*

	1	2	3	4	5	6	7	
Creative	☐	☐	☐	☐	☐	☐	☐	Dull

*

	1	2	3	4	5	6	7	
Easy to learn	☐	☐	☐	☐	☐	☐	☐	Difficult to learn

*

	1	2	3	4	5	6	7	
Valuable	☐	☐	☐	☐	☐	☐	☐	Inferior

*

1 2 3 4 5 6 7

Boring ☐ ☐ ☐ ☐ ☐ ☐ ☐ Exciting

*

1 2 3 4 5 6 7

Not interesting ☐ ☐ ☐ ☐ ☐ ☐ ☐ Interesting

*

1 2 3 4 5 6 7

Unpredictable ☐ ☐ ☐ ☐ ☐ ☐ ☐ Predictable

*

1 2 3 4 5 6 7

Fast ☐ ☐ ☐ ☐ ☐ ☐ ☐ Slow

*

1 2 3 4 5 6 7

Inventive ☐ ☐ ☐ ☐ ☐ ☐ ☐ Conventional

*

1 2 3 4 5 6 7

Obstructive ☐ ☐ ☐ ☐ ☐ ☐ ☐ Supportive

*

1 2 3 4 5 6 7

Good ☐ ☐ ☐ ☐ ☐ ☐ ☐ Bad

★

1 2 3 4 5 6 7

Complicated ☐ ☐ ☐ ☐ ☐ ☐ ☐ Easy

★

1 2 3 4 5 6 7

Unlikable ☐ ☐ ☐ ☐ ☐ ☐ ☐ Pleasing

★

1 2 3 4 5 6 7

Usual ☐ ☐ ☐ ☐ ☐ ☐ ☐ Leading Edge

★

1 2 3 4 5 6 7

Unpleasant ☐ ☐ ☐ ☐ ☐ ☐ ☐ Pleasant

★

1 2 3 4 5 6 7

Secure ☐ ☐ ☐ ☐ ☐ ☐ ☐ Not secure

★

1 2 3 4 5 6 7

Motivating ☐ ☐ ☐ ☐ ☐ ☐ ☐ Demotivating

★

1 2 3 4 5 6 7

Meets expectations ☐ ☐ ☐ ☐ ☐ ☐ ☐ Does not meet expectations

*		1	2	3	4	5	6	7	
	Inefficient	☐	☐	☐	☐	☐	☐	☐	Efficient

*		1	2	3	4	5	6	7	
	Clear	☐	☐	☐	☐	☐	☐	☐	Confusing

*		1	2	3	4	5	6	7	
	Impractical	☐	☐	☐	☐	☐	☐	☐	Practical

*		1	2	3	4	5	6	7	
	Organized	☐	☐	☐	☐	☐	☐	☐	Cluttered

*		1	2	3	4	5	6	7	
	Attractive	☐	☐	☐	☐	☐	☐	☐	Unattractive

*		1	2	3	4	5	6	7	
	Friendly	☐	☐	☐	☐	☐	☐	☐	Unfriendly

*		1	2	3	4	5	6	7	
	Conservative	☐	☐	☐	☐	☐	☐	☐	Innovative

Usability and Acceptance

Using this tool when using web platforms would increase my privacy awareness and protection. *

	1	2	3	4	5	
Completely Disagree	☐	☐	☐	☐	☐	Completely Agree

I find this tool useful in terms of privacy. *

	1	2	3	4	5	
Completely Disagree	☐	☐	☐	☐	☐	Completely Agree

Using the tool makes me feel confident in detecting and avoiding dark patterns. *

	1	2	3	4	5	
Completely Disagree	☐	☐	☐	☐	☐	Completely Agree

I would use this tool frequently when navigating the web. *

	1	2	3	4	5	
Completely Disagree	☐	☐	☐	☐	☐	Completely Agree

Appendix D

This appendix includes the full questionnaire results used in Chapter 07 to evaluate the Dark Patterns Detection Tool's usability, visual appeal, and effectiveness. The survey was distributed to users as part of the final evaluation phase, aiming to collect feedback on their overall experience with the tool.

 Αντιγραφή γραφήματος

Thank you for participating in this survey, which aims to evaluate the usability, clarity, and overall user experience of a tool designed to detect dark patterns in websites.

This research is non-commercial, and researchers receive no monetary benefits. Your responses are anonymous and will be used strictly for research purposes, including academic reports and publications. Please do not provide any personally identifiable information.

The survey takes approximately **5-10 minutes** and involves interacting with the tool and answering a short set of questions.

By completing this survey, you confirm that:

You understand the survey's purpose.

Participation is voluntary and you can withdraw at any time.

Your responses will be securely stored and only accessed by the research team.

For any questions or concerns, please contact:

Eleni Loizou (University of Cyprus) – eloizo06@ucy.ac.cy

Evangelia Vanezi (University of Cyprus) –
vanezievangelia@gmail.com

62 απαντήσεις

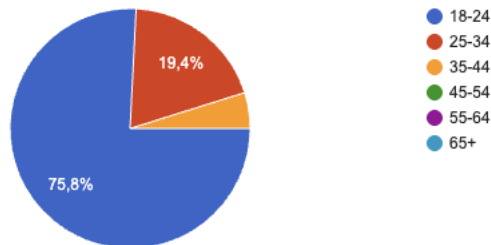


Background Information

What is your age group?

62 απαντήσεις

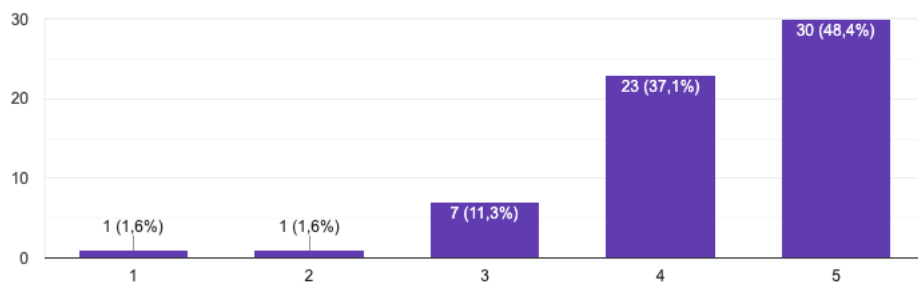
 Αντιγραφή γραφήματος



How would you describe your level of familiarity with technology and websites?

62 απαντήσεις

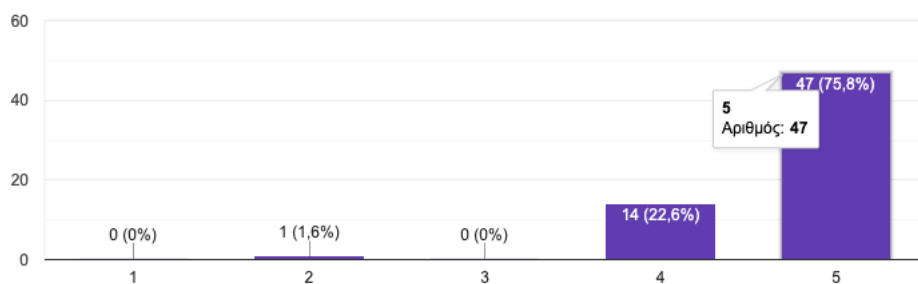
 Αντιγραφή γραφήματος



How often do you use websites or online services?

62 απαντήσεις

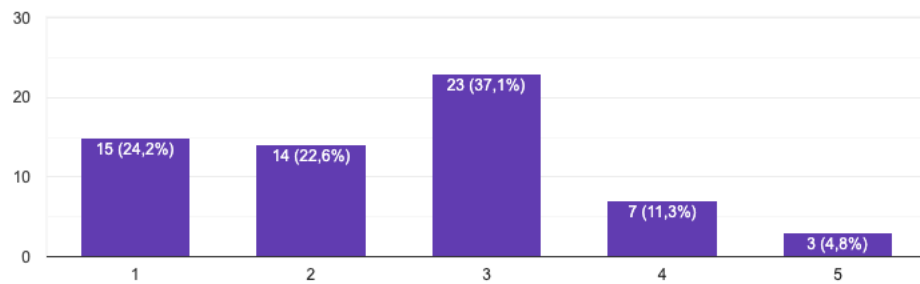
 Αντιγραφή γραφήματος



How would you describe your level of familiarity with the concept of 'dark patterns'?

Αντιγραφή γραφήματος

62 απαντήσεις



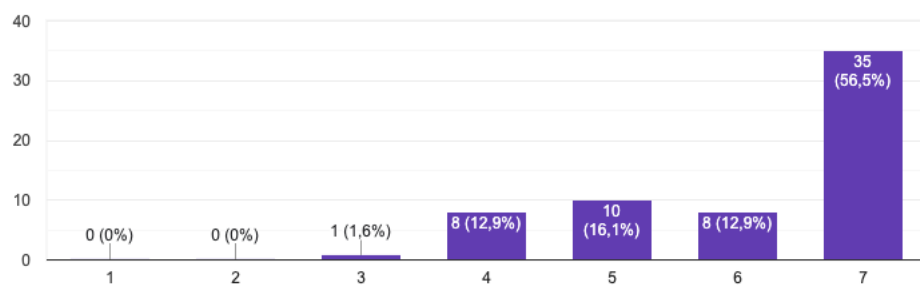
Dark Patterns Tool - Demo

You may also access and interact with the tool live using the following link: <https://students.cs.ucy.ac.cy/~eloizo06/index.html>.

User Experience Evaluation

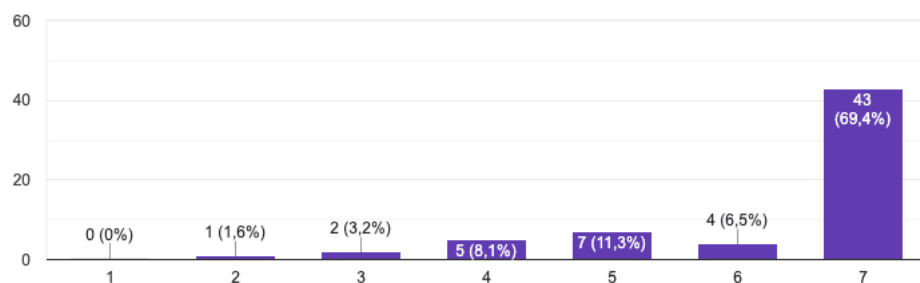
62 απαντήσεις

Αντιγραφή γραφήματος



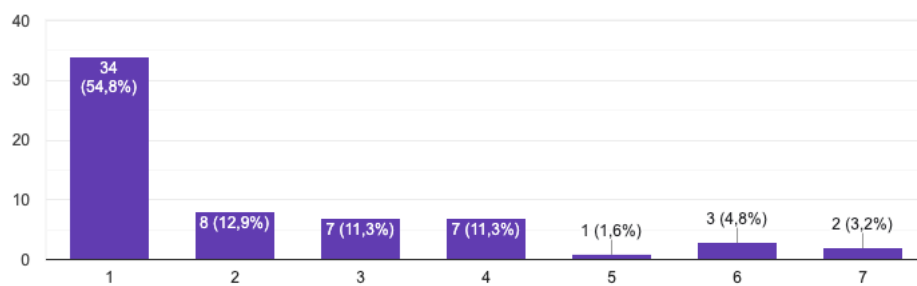
62 απαντήσεις

Αντιγραφή γραφήματος



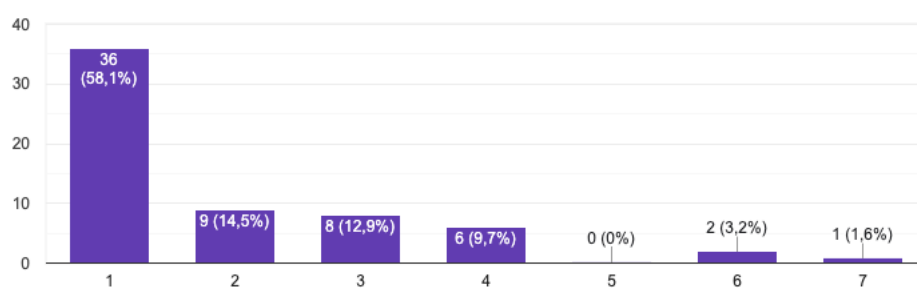
62 απαντήσεις

Αντιγραφή γραφήματος



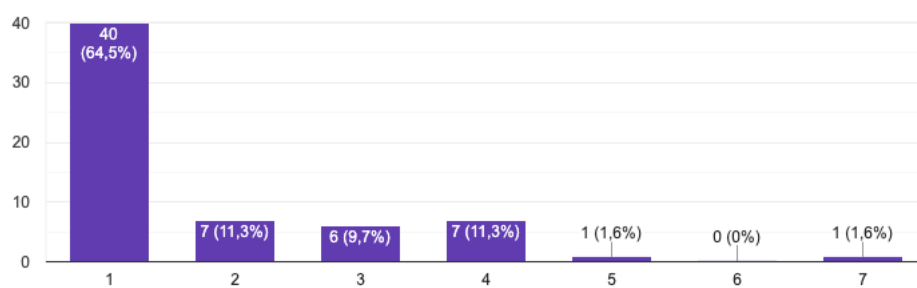
62 απαντήσεις

Αντιγραφή γραφήματος



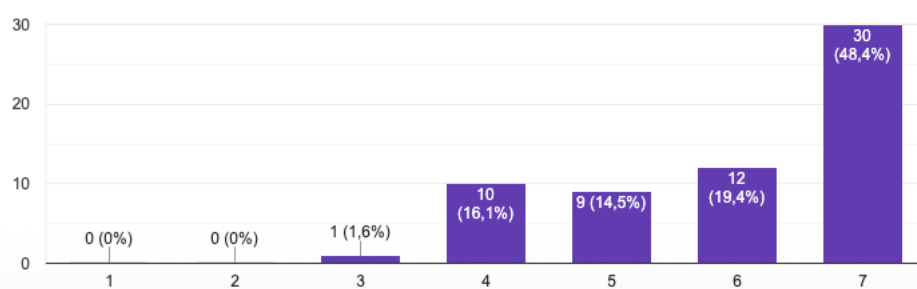
62 απαντήσεις

Αντιγραφή γραφήματος



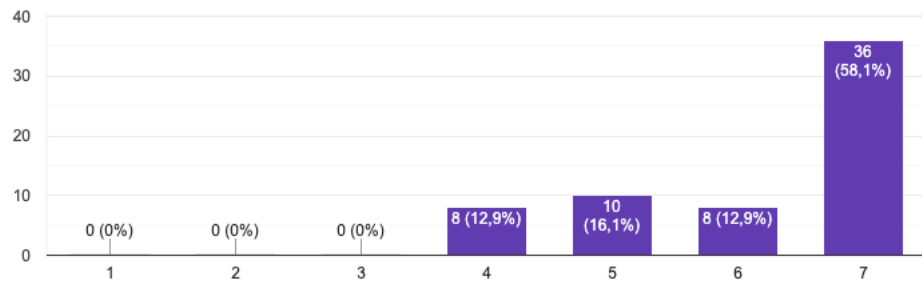
62 απαντήσεις

Αντιγραφή γραφήματος



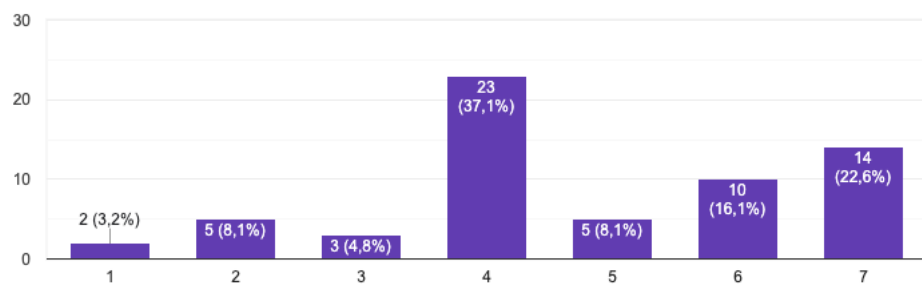
62 απαντήσεις

Αντιγραφή γραφήματος



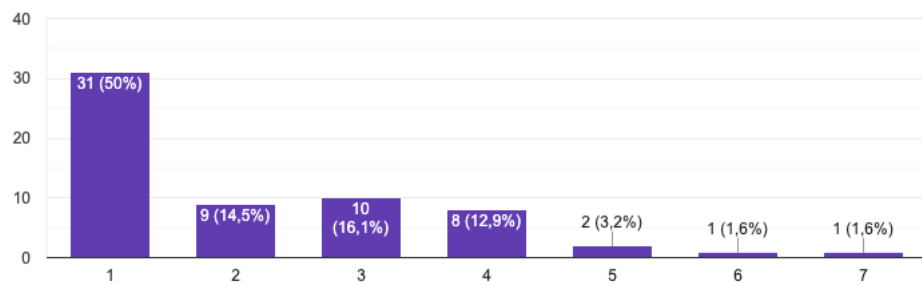
62 απαντήσεις

Αντιγραφή γραφήματος



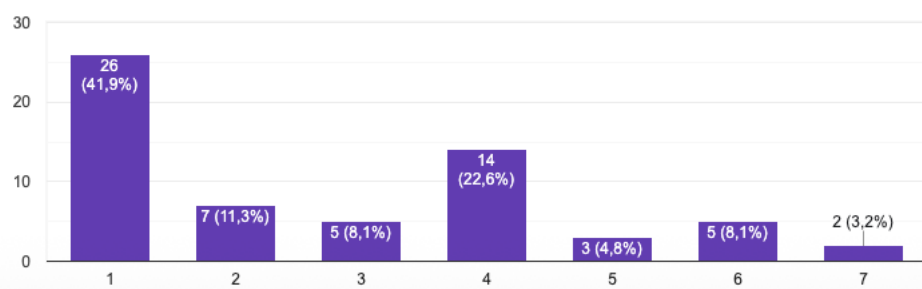
62 απαντήσεις

Αντιγραφή γραφήματος



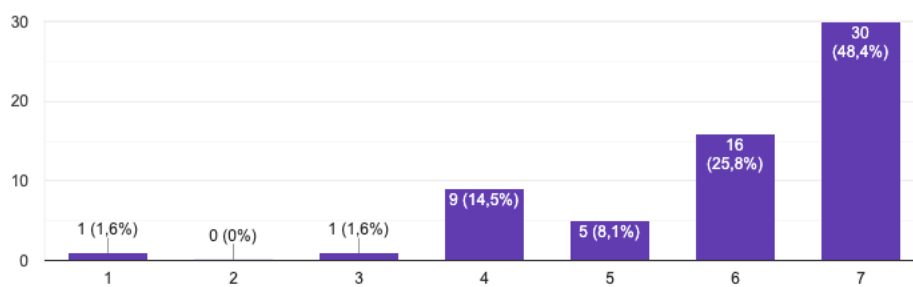
62 απαντήσεις

Αντιγραφή γραφήματος



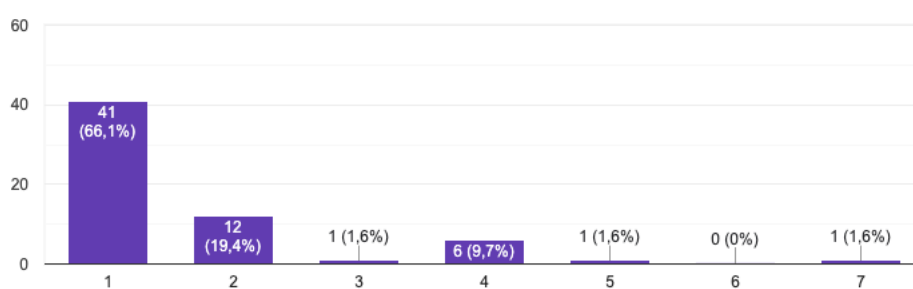
62 απαντήσεις

Αντιγραφή γραφήματος



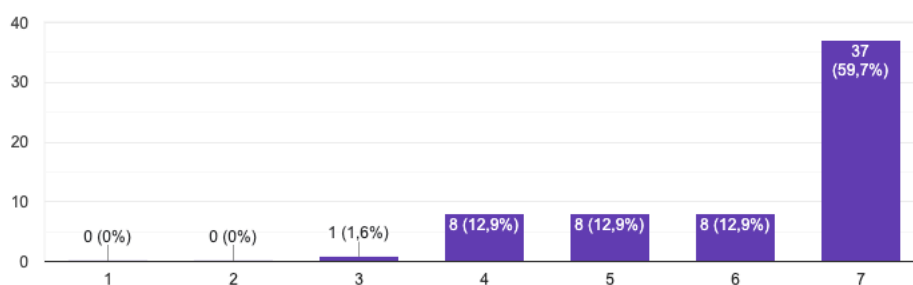
62 απαντήσεις

Αντιγραφή γραφήματος



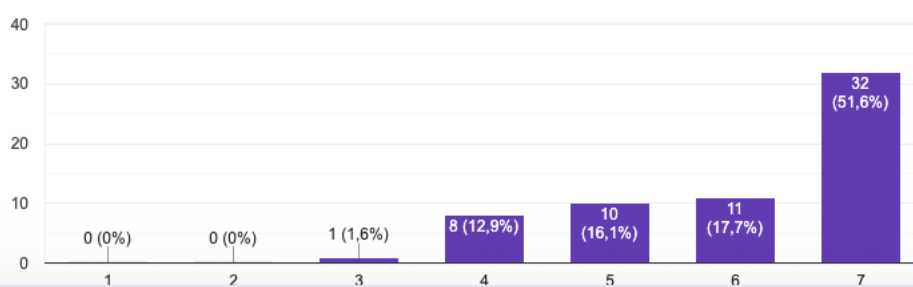
62 απαντήσεις

Αντιγραφή γραφήματος



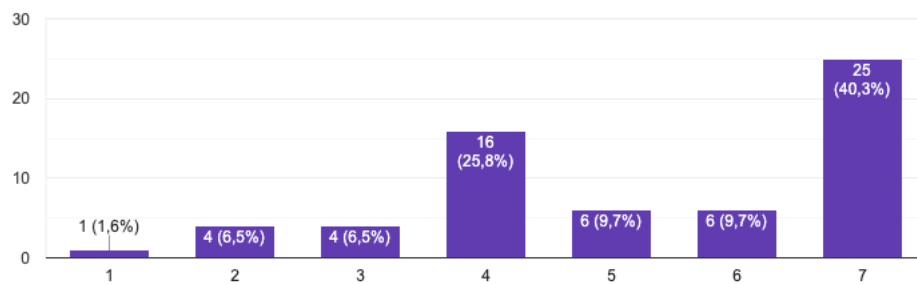
62 απαντήσεις

Αντιγραφή γραφήματος



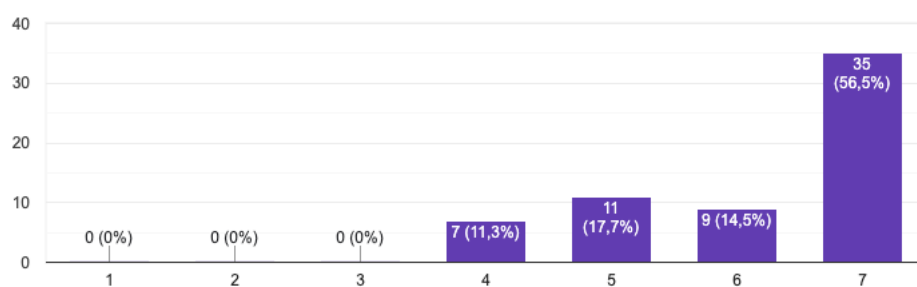
62 απαντήσεις

 Αντιγραφή γραφήματος



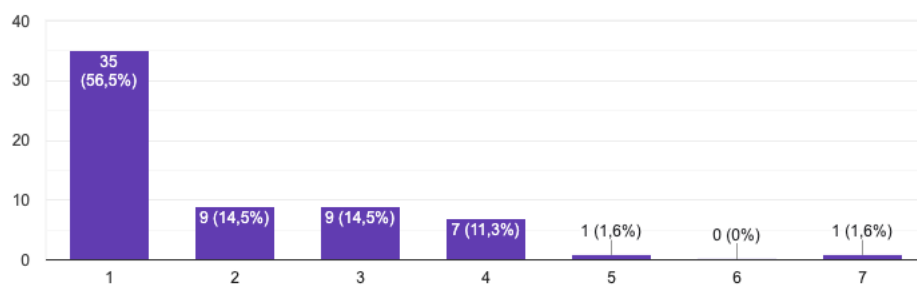
62 απαντήσεις

 Αντιγραφή γραφήματος



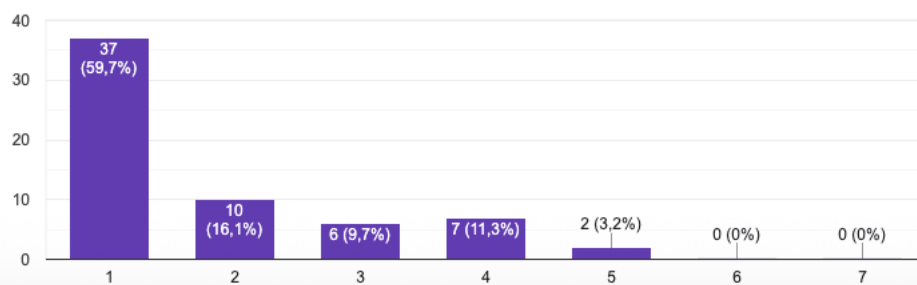
62 απαντήσεις

 Αντιγραφή γραφήματος



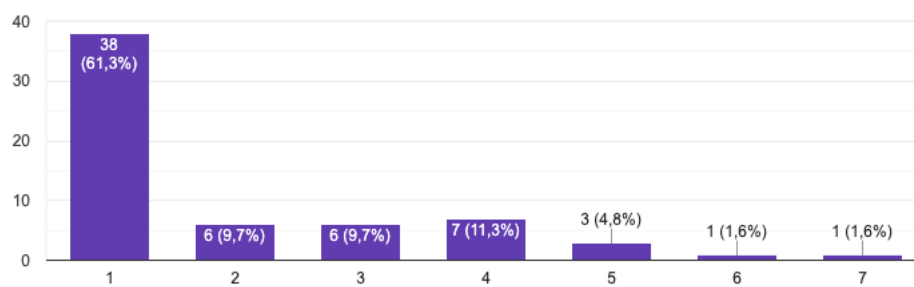
62 απαντήσεις

 Αντιγραφή γραφήματος



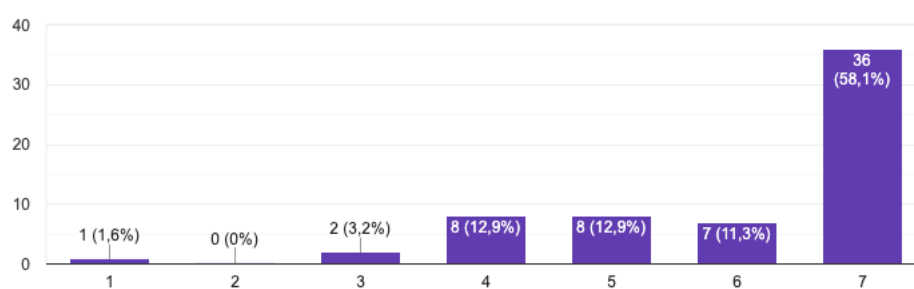
62 απαντήσεις

 Αντιγραφή γραφήματος



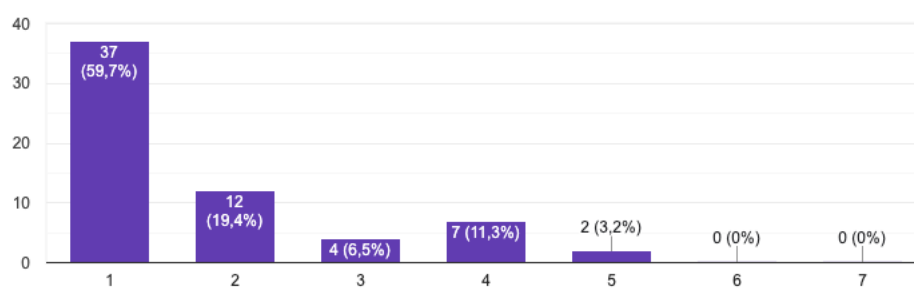
62 απαντήσεις

 Αντιγραφή γραφήματος



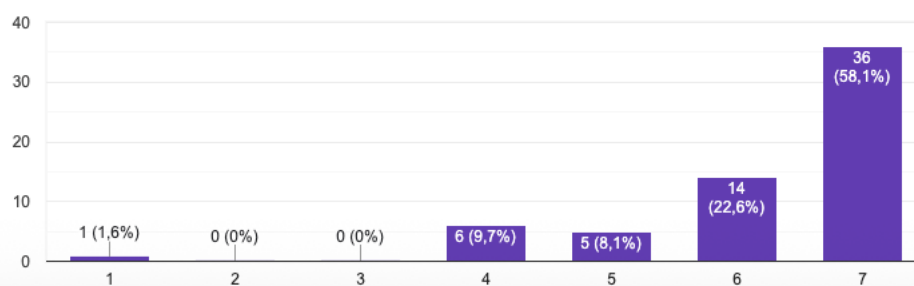
62 απαντήσεις

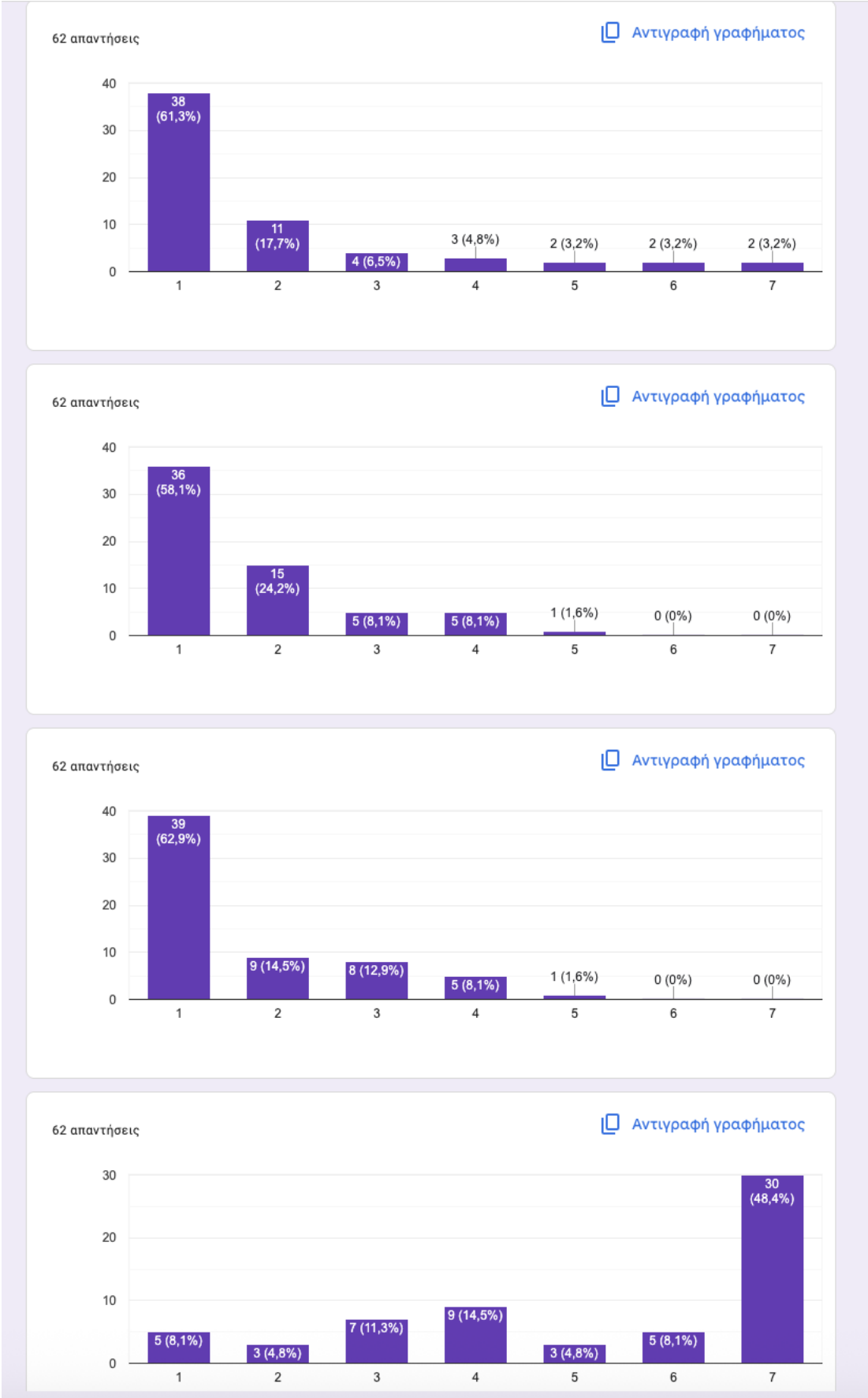
 Αντιγραφή γραφήματος



62 απαντήσεις

 Αντιγραφή γραφήματος



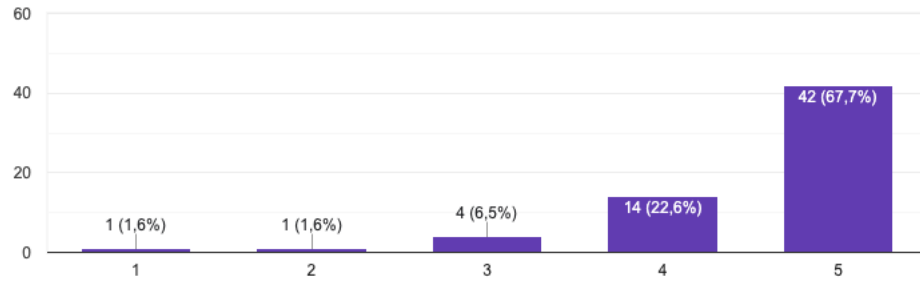


Usability and Acceptance

Using this tool when using web platforms would increase my privacy awareness and protection.

 Αντιγραφή γραφήματος

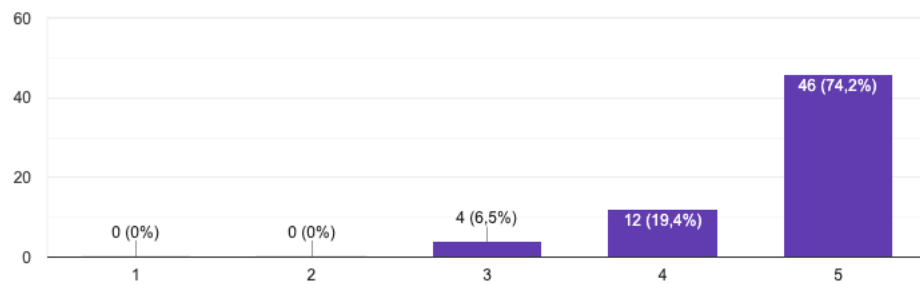
62 απαντήσεις



I find this tool useful in terms of privacy.

 Αντιγραφή γραφήματος

62 απαντήσεις

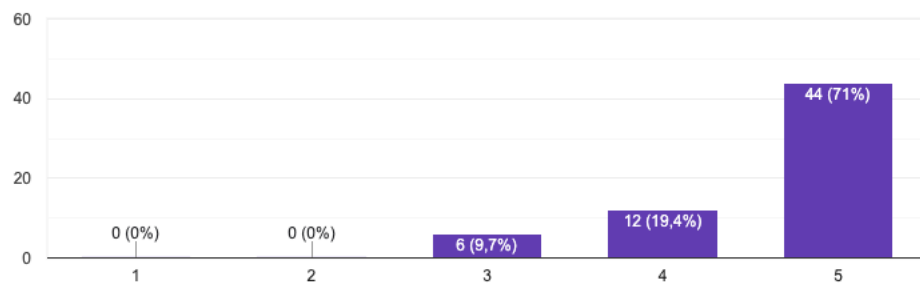


Using the tool makes me feel confident in detecting and avoiding dark patterns.

 Αντιγραφή γραφήματος

Αντιγραφή γραφήματος

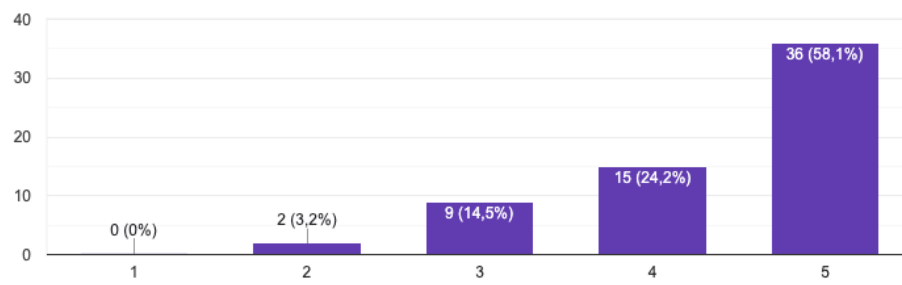
62 απαντήσεις



I would use this tool frequently when navigating the web.

 Αντιγραφή γραφήματος

62 απαντήσεις



Thank you / Exit Page

Thank you

Appendix E

This appendix includes the full Machine-Readable taxonomy mentioned in Chapter 04

```
[
  {
    "patternNumber": 1,
    "name": "Bad Defaults",
    "description": "The default options are sometimes chosen badly in a way that favors personal data processing or sharing.",
    "typicalInterfaceLocation": [
      "Cookie banners",
      "Registration forms",
      "Account settings"
    ],
    "observableIndications": [
      "Check whether any options are pre-selected by default",
      "Identify whether privacy-invasive settings are enabled by default and require users to opt out",
      "Assess whether the interface favors data-sharing choices through visual emphasis",
      "Check whether users are required to take additional steps to disable data collection or refuse consent",
      "Identify whether consent is implied due to the absence of a clear refusal option"
    ],
    "technicalIndicators": {
      "domHtml": {
        "description": [
          "Presence of checkbox inputs with the checked attribute enabled by default",
          "Data processing or preference options pre-selected without user interaction",
          "Absence of explicit opt-in mechanism"
        ],
        "codeExamples": [
          "<input id=\"persistent\" name=\"persistent\" type=\"checkbox\" checked>"
        ]
      },
      "cssLayout": {
        "description": [
          "Default-selected options are visually rendered as active",
          "The checked state is reinforced through CSS styling",
          "Privacy-protective alternatives are not equally emphasized visually"
        ],
        "codeExamples": [
          "input[type=checkbox]:checked + label::before"
        ]
      }
    }
  }
]
```

```

    ]
  },
  "javascriptBehavior": {
    "description": [
      "Default settings remain active unless the user manually changes them",
      "No user action results in the default option being applied",
      "The system behavior assumes acceptance unless the option is explicitly deselected"
    ],
    "codeExamples": [
      "if
(document.getElementById(\"persistent\").checked) {
keepUserLoggedIn(); }"
    ]
  },
  "gdprMapping": [
    "Article 25(2) - data protection by default, personal data processing and sharing should not be enabled by default"
  ],
  "prevalence": {
    "count": 22,
    "total": 217,
    "percentage": 10.14
  },
  "keywords": [
    "checked",
    "pre-selected",
    "preselected",
    "enabled by default",
    "selected by default",
    "default option",
    "opt out",
    "pre-ticked",
    "ticked by default"
  ]
},

```

```

{
  "patternNumber": 2,
  "name": "Hidden legalese stipulations",
  "description": "Services hide stipulations in the policies which target the privacy of the user.",
  "typicalInterfaceLocation": [
    "Cookie banners",
    "Registration forms",
    "Account settings",
    "Privacy and cookie policy pages"
  ],
  "observableIndications": [

```

```

        "Check whether information about data collection,
        third-party sharing, or tracking is explicitly stated in the
        initial banner or interface, rather than only in linked
        policies",
        "Identify whether key details (e.g., use of third
        parties, personalized advertising, sensitive data processing)
        are accessible only through secondary links such as "Privacy
        Policy" or "Cookie Policy",
        "Check whether important information is placed in low-
        visibility areas (e.g., footer links, small text below
        buttons, secondary layers) instead of the main consent
        interface",
        "Assess whether the language used is vague or non-
        specific (e.g., references to "partners," "other services," or
        "marketing purposes" without clear explanation)",
        "Identify whether users must navigate through multiple
        pages or clicks to understand how their data is collected,
        shared, or used"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Presence of privacy-related information only
                through secondary links (e.g., privacy statement, third-party
                cookies) rather than directly in the main consent text",
                "Key privacy details placed inside anchor elements
                linking to external or secondary policy pages",
                "Important information provided outside the main
                decision controls"
            ],
            "codeExamples": [
                "<a href=\"...\">Δήλωση προστασίας προσωπικών
                δεδομένων</a>",
                "<a href=\"...\">Cookies τρίτων μερών</a>"
            ]
        },
        "cssLayout": {
            "description": [
                "Privacy-related links are presented as secondary
                text links beneath the main consent controls",
                "Primary action buttons are visually more
                prominent than links to privacy information",
                "Important privacy information is placed in a
                lower-visibility area of the banner"
            ],
            "codeExamples": [
                ".policy-link { font-size: 14px; text-decoration:
                underline; }",
                ".accept-btn { font-size: 18px; font-weight: bold;
            }"
            ]
        },
        "javascriptBehavior": {
            "description": [

```

```

        "Users can make a consent decision without opening
the linked privacy information",
        "Accessing key privacy details requires additional
navigation through external or secondary pages",
        "The interface does not force prior review of the
linked privacy information before consent"
    ],
    "codeExamples": [
        "acceptButton.addEventListener(\"click\", () => {
saveConsent(\"accepted\"); });"
    ]
},
"gdprMapping": [
    "Article 12(1) - information must be provided in a
concise, transparent, intelligible and easily accessible form,
using clear and plain language; however, key privacy
information is hidden in policies or secondary layers."
],
"prevalence": {
    "count": 16,
    "total": 217,
    "percentage": 7.37
},
"keywords": [
    "privacy policy",
    "cookie policy",
    "terms",
    "third parties",
    "third-party cookies",
    "partners",
    "data sharing",
    "personalized advertising"
]
},

```

```

{
    "patternNumber": 3,
    "name": "Ease",
    "description": "User interface focuses on the positive
aspects of one choice while glossing over any potentially
negative aspects, leading many users to comply with the
service provider's wishes.",
    "typicalInterfaceLocation": [
        "Cookie banners"
    ],
    "observableIndications": [
        "Check whether the interface emphasizes the benefits
of accepting (e.g., \"improve your experience\", \"personalized
content\", \"relevant ads\") while omitting or downplaying
potential risks (e.g., tracking, data sharing)",
    ]
}

```

```

        "Identify whether positive or reassuring language
(e.g., "better experience", "trust", "safety") is used to
frame consent, without clearly explaining the implications",
        "Assess whether privacy-related consequences (e.g.,
tracking, third-party data use, personalization) are not
equally visible or are less prominently presented than the
benefits",
        "Check whether accepting the option (e.g., "Accept
all", "Continue") is presented as the easiest, fastest, or
most convenient action, while alternative options require more
effort",
        "Identify whether the interface creates cognitive
overload (e.g., long or complex explanations) that distracts
from understanding the negative implications of the choice"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Presence of benefit-oriented language in the
main consent text (e.g., "improve your experience",
"personalized advertising")",
                "Privacy-invasive practices (e.g., tracking,
advertising) described using positive framing",
                "Lack of clear and direct mention of potential
privacy risks in the main text"
            ],
            "codeExamples": [
                "<p>We use optional cookies to improve your
experience on our websites and to display personalized
advertising based on your online activity.</p>"
            ]
        },
        "cssLayout": {
            "description": [
                "Benefit-oriented text is placed prominently
within the main consent message",
                "No visual distinction or emphasis is given to
potential privacy risks",
                "The consent description appears neutral or
positive without highlighting negative implications"
            ],
            "codeExamples": [
                ".consent-text { color: #333; font-size: 14px;
}"
            ]
        },
        "javascriptBehavior": {
            "description": [
                "Users can accept consent directly without being
exposed to detailed privacy implications",
                "No additional interaction is required to reveal
potential risks",
                "The interface allows immediate acceptance based
on positively framed information"
            ]
        }
    }
}

```

```

    ],
    "codeExamples": [
      "acceptButton.addEventListener(\"click\", () =>
{ enableOptionalCookies(); });"
    ]
  },
  "gdprMapping": [
    "Article 7(4) - consent must be freely given and not
influenced by interface design; however, the interface
emphasizes benefits and downplays risks, steering users toward
accepting data processing."
  ],
  "prevalence": {
    "count": 40,
    "total": 217,
    "percentage": 18.43
  },
  "keywords": [
    "better experience",
    "improve your experience",
    "personalized content",
    "personalized recommendations",
    "relevant ads",
    "tailored offers",
    "relevant content"
  ]
},

```

```

{
  "patternNumber": 4,
  "name": "Impenetrable wall",
  "description": "User interface that blocks access to a
service through a cookie wall or account creation requirement,
even when this is not necessary to use the service.",
  "typicalInterfaceLocation": [
    "Initial website access (first page load pop-up)"
  ],
  "observableIndications": [
    "Check whether access is blocked immediately upon
visiting the website (e.g., a cookie wall or registration gate
appears on the first page load)",
    "Check whether access to the website or core content
is blocked until the user accepts cookies, terms, or data
processing"
  ],
  "technicalIndicators": {
    "domHtml": {
      "description": [
        "Presence of modal or overlay elements (e.g.,
div.modal, div.notice) that block access to page content",
        "Main content is visually and structurally
placed behind the consent layer",

```

```

        "Consent interface presented as a blocking layer
before accessing the service"
    ],
    "codeExamples": [
        "<div id=\"notice\" class=\"message type-
modal\"><button>Accept all</button></div>"
    ]
},
"cssLayout": {
    "description": [
        "Overlay covers the full viewport and blocks
interaction with background content",
        "Background content is dimmed or visually
inaccessible",
        "Modal is centered and visually dominant with
higher z-index"
    ],
    "codeExamples": [
        ".modal { position: fixed; z-index: 9999; width:
100%; height: 100%; }"
    ]
},
"javascriptBehavior": {
    "description": [
        "Page interaction is blocked until the user
makes a consent decision",
        "Scrolling or clicking background content is
disabled",
        "Access to content is conditional on accepting
cookies or selecting an alternative option (e.g.,
subscription)"
    ],
    "codeExamples": [
        "if (!consentGiven) { showModal();
document.body.style.overflow = \"hidden\"; }"
    ]
},
},
"gdprMapping": [
    "Article 7(4) - consent must be freely given;
however, access to the service is made conditional on
consenting to data processing that is not necessary for using
the service."
],
"prevalence": {
    "count": 10,
    "total": 217,
    "percentage": 4.61
},
"keywords": [
    "accept to continue",
    "required to access",
    "continue to access",
    "must accept",

```

```

        "subscribe to continue",
        "block access"
    ]
},

```

```

{
    "patternNumber": 5,
    "name": "Last minute consent",
    "description": "Involves seeking consent for the
collection of data at a specific moment where the user is in a
weak position, such as being in a hurry or impatient to
complete an action.",
    "typicalInterfaceLocation": [],
    "observableIndications": [],
    "technicalIndicators": {
        "domHtml": {
            "description": [],
            "codeExamples": []
        },
        "cssLayout": {
            "description": [],
            "codeExamples": []
        },
        "javascriptBehavior": {
            "description": [],
            "codeExamples": []
        }
    },
    "gdprMapping": [
        "Article 7(4) - consent must be freely given;
however, consent is requested at a moment where the user is
under time pressure, reducing the ability to make a free and
informed decision."
    ],
    "prevalence": {
        "count": 0,
        "total": 217,
        "percentage": 0.0
    },
    "keywords": []
},

```

```

{
    "patternNumber": 6,
    "name": "Pressure to allow permissions",
    "description": "Not allowing the use of a service
unless multiple permissions are granted (e.g., access to the
camera, microphone, or GPS).",
    "typicalInterfaceLocation": [
        "Registration process"
    ],
    "observableIndications": [

```

```

        "Identify whether access or full functionality is
        conditioned on granting permissions (e.g., third-party login,
        tracking, or location access)",
        "Assess whether the interface implies reduced
        functionality, limited features, or restricted access if
        permissions are denied"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Presence of consent or permission text stating
                that certain features require enabling tracking,
                personalization, or permissions",
                "Permission-related options presented as
                necessary to continue or access functionality",
                "Lack of an equally accessible alternative path
                without granting permissions or consent"
            ],
            "codeExamples": [
                "<p>Enable location access to continue</p>",
                "<p>Accept cookies to access all features</p>"
            ]
        },
        "cssLayout": {
            "description": [
                "Permission or consent request displayed
                prominently within the main interface or consent banner",
                "Main action to allow permissions/consent
                visually emphasized more than refusal or skip options",
                "Warning or limitation text placed near the
                primary action button"
            ],
            "codeExamples": [
                ".allow-btn { font-weight: bold; }",
                ".permission-text { color: #333; }"
            ]
        },
        "javascriptBehavior": {
            "description": [
                "Users cannot access the full service or certain
                features unless permissions or consent are granted",
                "Denying permission leads to restricted
                functionality or repeated prompts",
                "No equivalent, equally easy fallback is
                provided without granting permission"
            ],
            "codeExamples": [
                "if (!consentGiven) { restrictFeatures(); }"
            ]
        }
    },
    "gdprMapping": [
        "Article 7(4) - consent must be freely given;
        however, access to the service or its full functionality is

```

made conditional on granting permissions or data processing that may not be necessary for the service."

```
    ],
    "prevalence": {
      "count": 5,
      "total": 217,
      "percentage": 2.30
    },
    "keywords": [
      "enable location access",
      "allow location",
      "enable camera",
      "allow camera",
      "enable microphone",
      "allow microphone",
      "grant permission",
      "access all features",
      "permission required",
      "required permission",
      "enable permissions",
      "allow permissions"
    ]
  },
}
```

```
{
  "patternNumber": 7,
  "name": "Pressure to receive marketing",
  "description": "Requiring the data subject to agree to receive marketing offers by email in order to complete a purchase or sign up.",
  "typicalInterfaceLocation": [
    "Cookie banners",
    "Registration process"
  ],
  "observableIndications": [
    "Check whether the registration or checkout form includes a pre-selected checkbox for receiving marketing emails",
    "Identify whether users are automatically enrolled in marketing communications during sign-up without an explicit opt-in step",
    "Check whether the only way to avoid marketing emails is to manually uncheck an option (opt-out instead of opt-in)",
    "Assess whether the marketing consent option is presented as part of required steps to complete registration or purchase",
    "Identify whether the checkbox uses negative or confusing wording (e.g., \"Please do not email me\") that makes the user more likely to consent unintentionally"
  ],
  "technicalIndicators": {
    "domHtml": {
```

```

        "description": [
            "Presence of marketing-related checkbox inputs
(e.g., marketingOptIn)",
            "Checkbox is pre-selected using the checked
attribute",
            "Marketing consent is enabled by default without
explicit user action"
        ],
        "codeExamples": [
            "<input type=\"checkbox\"
id=\"paypalAccountData_marketingOptIn\" checked>"
        ]
    },
    "cssLayout": {
        "description": [
            "Marketing consent checkbox appears visually
selected (checked state)",
            "No visual emphasis indicates that this option
is optional or not required",
            "The checked state is visually reinforced
through UI elements (e.g., checkmark icon)"
        ],
        "codeExamples": [
            "input[type=checkbox]:checked { accent-color:
blue; }"
        ]
    },
    "javascriptBehavior": {
        "description": [
            "Users are automatically enrolled in marketing
communications unless they manually deselect the checkbox",
            "No explicit opt-in action is required to
receive marketing",
            "The system assumes consent unless the user
actively opts out"
        ],
        "codeExamples": [
            "if (marketingCheckbox.checked) {
enableMarketingEmails(); }"
        ]
    },
    "gdprMapping": [
        "Article 7(4) - consent must be freely given;
however, marketing consent is required to complete
registration or purchase.",
        "Article 7(2) - consent must be clearly
distinguishable; however, marketing consent is embedded within
the sign-up flow."
    ],
    "prevalence": {
        "count": 7,
        "total": 217,
        "percentage": 3.23
    }
}

```

```

    },
    "keywords": [
      [
        "marketing",
        "newsletter",
        "promotional offers",
        "email updates",
        "product updates",
        "marketing emails",
        "promotional emails",
        "marketing communications",
        "receive marketing",
        "marketing opt in"
      ]
    ]
  },
  {
    "patternNumber": 8,
    "name": "Pressure to confirm",
    "description": "Using negative persuasive language to make a data subject feel bad about not accepting a certain modality of data collection.",
    "typicalInterfaceLocation": [
      "Delete account process"
    ],
    "observableIndications": [
      "Check whether the interface displays warning messages when the user tries to disable data processing, delete an account, or refuse consent (e.g., pop-ups or confirmation screens)",
      "Identify whether these messages emphasize loss of features, access, or benefits (e.g., \"you may lose access\", \"your experience will be affected\")",
      "Check whether fear-based or negatively framed language is used to discourage the user from proceeding (e.g., highlighting risks without balanced explanation)",
      "Assess whether the confirmation message is emotionally persuasive (e.g., guilt-inducing tone, discouraging wording) rather than neutral"
    ],
    "technicalIndicators": {
      "domHtml": {
        "description": [
          "Presence of confirmation modal with negatively framed button labels",
          "Use of emotionally persuasive language within button text (e.g., \"No, take me back!\")",
          "Unequal wording between confirmation and cancellation options"
        ]
      },
      "codeExamples": [
        "<button>No, take me back!</button>",

```

```

        "<button>Yes, I'm sure</button>"
    ],
    },
    "cssLayout": {
        "description": [
            "Confirmation button visually emphasized (e.g.,
colored, bold styling)",
            "Secondary option is less prominent and
negatively framed",
            "Modal dialog is centrally positioned and
visually dominant"
        ],
        "codeExamples": [
            ".confirm-btn { background-color: red; }",
            ".cancel-btn { background-color: gray; }"
        ]
    },
    "javascriptBehavior": {
        "description": [
            "Additional confirmation step is required before
disabling data processing",
            "User must interact with the modal before
completing the action",
            "Flow interruption discourages opting out"
        ],
        "codeExamples": [
            "confirmButton.addEventListener(\"click\",
disableDataProcessing);"
        ]
    },
    },
    "gdprMapping": [
        "Article 7(4) - consent must be freely given;
however, the interface uses negative and persuasive language
to influence the user's decision.",
        "Article 5(1)(a) - processing must be fair; however,
the interface applies manipulative and guilt-inducing
wording."
    ],
    "prevalence": {
        "count": 3,
        "total": 217,
        "percentage": 1.38
    },
    "keywords": [
        "no, take me back",
        "are you sure",
        "you may lose access",
        "your experience will be affected",
        "go back",
        "stay subscribed",
        "no, i prefer",
        "worse experience"
    ]
]

```

```

    },
    {
        "patternNumber": 9,
        "name": "Difficult deletion",
        "description": "Making it difficult or inconvenient to delete the user account.",
        "typicalInterfaceLocation": [
            "Delete account process"
        ],
        "observableIndications": [
            "Check whether the account deletion option is clearly visible and accessible within the account settings (e.g., not hidden across multiple pages)",
            "Identify whether deleting the account requires multiple steps (e.g., navigating through several pages, repeated confirmations, or entering additional information)",
            "Check whether deletion requires actions outside the platform (e.g., sending an email to support or completing external verification)",
            "Assess whether the interface offers deactivation instead of full deletion, making permanent account removal unclear or harder to achieve",
            "Identify whether account deletion does not automatically remove personal data and requires additional requests to fully erase user information"
        ],
        "technicalIndicators": {
            "domHtml": {
                "description": [
                    "Presence of a \"Delete account\" option only after multiple navigation steps",
                    "Account deletion functionality split across several pages or forms",
                    "Deletion is available, but not directly accessible from the main account settings"
                ],
                "codeExamples": [
                    "<a href=\"/settings/account\">Account settings</a>",
                    "<a href=\"/settings/account/delete\">Delete account</a>"
                ]
            },
            "cssLayout": {
                "description": [
                    "Delete option is placed in low-visibility sections or deeper settings layers",
                    "Account deletion control is visually de-emphasized compared to other account actions",
                    "Important deletion steps are distributed across multiple screens"
                ],
                "codeExamples": [

```

```

        ".delete-link { font-size: 12px; color: #777; }"
    ],
    },
    "javascriptBehavior": {
        "description": [
            "Multiple confirmation steps are required before
deletion is completed",
            "Additional verification or external
confirmation is required",
            "Deletion process introduces friction before
completion"
        ],
        "codeExamples": [
            "function deleteAccount() {
showConfirmationStep1(); sendEmailVerification(); }"
        ]
    },
    },
    "gdprMapping": [
        "Article 17 - the data subject has the right to
obtain erasure of personal data; however, account deletion is
made difficult or inaccessible.",
        "Article 12(2) - the controller shall facilitate the
exercise of data subject rights; however, deletion requires
multiple steps or external actions."
    ],
    "prevalence": {
        "count": 12,
        "total": 217,
        "percentage": 5.53
    },
    "keywords": [
        "delete account",
        "deactivate account",
        "close account",
        "contact support",
        "send us an email",
        "request deletion",
        "verification"
    ]
}
},

```

```

{
    "patternNumber": 10,
    "name": "Hidden Settings",
    "description": "Hiding privacy settings in places that
are not intuitive or that require the data subject to navigate
through multiple drop-down choices to access them.",
    "typicalInterfaceLocation": [
        "Cookie banners"
    ],
    "observableIndications": [
        "Check whether privacy controls (e.g., cookie
preferences, personalization settings, data sharing options)

```

```

are hidden behind expandable sections (e.g., "Customize",
"Manage preferences")",
    "Identify whether users must navigate through
multiple layers (e.g., "Show purposes", partner lists,
additional settings pages) to access or modify privacy
settings",
    "Check whether key options (e.g., "Reject",
"Decline", or granular controls) are not available on the
first layer and require additional clicks to access",
    "Assess whether accepting consent (e.g., "Accept
all") is immediately accessible, while managing or limiting
consent requires navigating deeper into the interface"
],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Presence of privacy controls inside nested or
collapsible elements (e.g., <details>, dropdowns, tabs)",
                "Privacy settings accessible only through
secondary buttons (e.g., "Manage", "Customize")",
                "Absence of direct access to privacy options in
the first interface layer"
            ],
            "codeExamples": [
                "<button>Manage cookies</button>",
                "<details><summary>Show
purposes</summary><div>Analytics,
Marketing...</div></details>"
            ]
        },
        "cssLayout": {
            "description": [
                "Privacy settings are hidden behind expandable
sections or tabs",
                "Controls are not visible in the default view
and require interaction to appear",
                "Primary actions (e.g., "Accept") are more
prominent than settings"
            ],
            "codeExamples": [
                ".hidden-settings { display: none; }"
            ]
        },
        "javascriptBehavior": {
            "description": [
                "Additional user interaction is required to
reveal privacy controls (e.g., click "Manage")",
                "Settings are dynamically displayed only after
interaction",
                "Multiple steps are required to access granular
controls"
            ],
            "codeExamples": [

```

```

        "manageBtn.addEventListener(\"click\", () => {
document.querySelector(\".hidden-settings\").style.display =
\"block\"; });"
    ]
    }
},
"gdprMapping": [
    "Article 25(1) - data protection by design requires
integrating privacy safeguards into the interface; however,
privacy settings are hidden and not easily accessible.",
    "Article 12(2) - the controller shall facilitate the
exercise of data subject rights; however, accessing privacy
controls requires multiple steps and navigation."
],
"prevalence": {
    "count": 9,
    "total": 217,
    "percentage": 4.15
},
"keywords": [
    "manage preferences",
    "cookie settings",
    "privacy settings",
    "manage cookies",
    "show purposes",
    "show partners",
    "customize choices",
    "manage settings"
]
},

```

```

{
    "patternNumber": 11,
    "name": "Ambiguity",
    "description": "Using confusing or ambiguous language
(e.g., double negatives) that makes it unclear what user
choices mean, such as whether data will be shared or not.",
    "typicalInterfaceLocation": [
        "Cookie consent interfaces",
        "Preference management panels",
        "Registration forms",
        "Consent pop-ups"
    ],
    "observableIndications": [
        "Check whether options (e.g., checkboxes or buttons)
use negative or double-negative phrasing (e.g., \"No, I do not
want...\") that may confuse the user",
        "Identify whether it is unclear what each option
means (e.g., whether selecting \"Yes\" or \"No\" results in data
sharing or refusal)",
        "Assess whether the wording of consent or rejection
options is ambiguous or non-specific (e.g., unclear what data
processing is accepted or declined)"
    ],

```

```

    "technicalIndicators": {
      "domHtml": {
        "description": [
          "Presence of consent options using negative or double-negative wording inside the input label or aria-label",
          "Checkbox meaning depends on interpreting a negatively phrased sentence rather than a direct action",
          "Consent/refusal wording embedded directly in the control text, making the outcome unclear"
        ],
        "codeExamples": [
          "<input type=\"checkbox\" aria-label=\"No, I do not want to receive marketing communications from Notion.\">",
          "<label>No, I do not want to receive marketing communications from Notion.</label>"
        ]
      },
      "cssLayout": {
        "description": [
          "Checkbox and label are displayed as a normal single control without additional clarification of what checked/unchecked means",
          "No visual aid is provided to distinguish consent from refusal beyond the ambiguous label text",
          "Small inline label text may increase the chance of misreading the option"
        ],
        "codeExamples": [
          ".label { font-size: 12px; font-weight: 400; }"
        ]
      },
      "javascriptBehavior": {
        "description": [
          "The effect of the control depends on whether the checkbox is checked or unchecked, but the wording does not make that state immediately clear",
          "Users must interpret the negative phrasing before understanding the result of their action",
          "The interface does not provide a clearer alternative wording for the same preference"
        ],
        "codeExamples": [
          "if (checkbox.checked) {
disableMarketingEmails(); } else { enableMarketingEmails(); }"
        ]
      },
      "gdprMapping": [
        "Article 12(1) - information must be provided in a clear and plain language; however, the interface uses ambiguous wording that makes user choices unclear.",
        "Article 7(2) - consent must be presented clearly and in an intelligible form; however, the meaning of the options is confusing or unclear."
      ]
    }
  }

```

```

    ],
    "prevalence": {
      "count": 2,
      "total": 217,
      "percentage": 0.92
    },
    "keywords": [
      "no, i do not want",
      "do not want",
      "not receive marketing",
      "please do not email me",
      "do not receive",
      "double negative"
    ]
  },

```

```

{
  "patternNumber": 12,
  "name": "Twist",
  "description": "Using colors and symbols in a way that
differs from customary design conventions in order to misguide
the data subject.",
  "typicalInterfaceLocation": [
    "Cookie banners"
  ],
  "observableIndications": [
    "Assess whether visual design elements (e.g., color
coding, button styling) guide the user toward accepting rather
than rejecting",
    "Check whether colors or visual cues are used in a
non-standard or misleading way (e.g., green for accept, grey
or hidden styling for reject)"
  ],
  "technicalIndicators": {
    "domHtml": {
      "description": [
        "Presence of multiple action buttons or icons
representing opposite choices (e.g., accept vs reject)",
        "Use of icons, labels, or button groupings that
do not clearly match the expected meaning of the action",
        "Visual decision elements are present, but their
semantics depend mainly on color or icon interpretation"
      ],
      "codeExamples": [
        "<button class=\"accept-btn\">Accept</button>",
        "<button class=\"reject-btn\">Reject</button>"
      ]
    },
    "cssLayout": {
      "description": [
        "Non-standard color mapping is used for choices
(e.g., green for reject, red for accept)",
        "Visual cues such as color, icon style, or
emphasis suggest the opposite of the actual action",

```

```

        "The visual hierarchy misguides the user by
making one option appear safer or more intuitive than it
really is"
    ],
    "codeExamples": [
        ".accept-btn { background-color: red; }",
        ".reject-btn { background-color: green; }"
    ]
},
"javascriptBehavior": {
    "description": [
        "Clicking a visually reassuring option triggers
a different or less expected outcome than the user may infer
from its styling",
        "User decisions rely on misleading visual cues
rather than clear semantic presentation",
        "The interface behavior reinforces a misleading
visual mapping between appearance and action"
    ],
    "codeExamples": [
        "document.querySelector(\".accept-
btn\").addEventListener(\"click\", enableTracking);",
        "document.querySelector(\".reject-
btn\").addEventListener(\"click\", disableTracking);"
    ]
},
"gdprMapping": [
    "Article 5(1)(a) - personal data must be processed
in a fair and transparent manner; however, the interface uses
misleading colors and visual cues that guide users toward
unintended choices.",
    "Article 7(2) - consent must be clearly presented;
however, visual design elements create confusion about the
available options."
],
"prevalence": {
    "count": 4,
    "total": 217,
    "percentage": 1.84
},
"keywords": [
    "accept",
    "reject",
    "green",
    "red",
    "misleading color",
    "visual cue"
]
},
{
    "patternNumber": 13,
    "name": "Obfuscation",

```

```

        "description": "Adding elements to a privacy setting
that are not connected to privacy, so that privacy information
becomes obfuscated.",
        "typicalInterfaceLocation": [
            "Cookie banners"
        ],
        "observableIndications": [
            "Check whether unrelated or excessive information is
included in the same section, making it difficult to identify
relevant privacy controls",
            "Identify whether the structure of the interface
(e.g., grouping, labeling, layout) makes it unclear how
personal data is processed and by whom"
        ],
        "technicalIndicators": {
            "domHtml": {
                "description": [
                    "Multiple data processing purposes are grouped
within the same control or section (e.g., analytics,
marketing, functionality combined)",
                    "Lack of clear structural separation between
different categories of data use",
                    "Privacy-related information is mixed with
general or unrelated interface content"
                ],
                "codeExamples": [
                    "<div class=\"consent-section\"><p>We use data
for analytics, personalization, and service
improvements.</p></div>"
                ]
            },
            "cssLayout": {
                "description": [
                    "Information is presented as long, dense text
blocks without clear segmentation",
                    "No visual grouping or hierarchy distinguishes
different data processing purposes",
                    "Multiple elements are displayed in a uniform
style, making it difficult to differentiate categories"
                ],
                "codeExamples": [
                    ".consent-section { font-size: 14px; line-
height: 1.5; }"
                ]
            },
            "javascriptBehavior": {
                "description": [
                    "A single interaction controls multiple data
processing purposes simultaneously",
                    "No granular control is provided over individual
data uses",
                    "User actions affect multiple processing
activities without clear distinction"
                ],
            },
        },
    },

```

```

        "codeExamples": [
            "consentCheckbox.addEventListener(\"change\", ()
=> { enableAnalytics(); enableAds(); enablePersonalization();
});"
        ]
    },
    "gdprMapping": [
        "Article 12(1) - information must be provided in a
concise, transparent, intelligible form; however, privacy
information is mixed with unrelated elements, reducing
clarity.",
        "Article 5(1)(a) - processing must be fair and
transparent; however, the interface obscures privacy-relevant
information through complex and cluttered presentation."
    ],
    "prevalence": {
        "count": 2,
        "total": 217,
        "percentage": 0.92
    },
    "keywords": [
        "analytics",
        "marketing",
        "personalization",
        "service improvements",
        "combined purposes",
        "same section"
    ]
}
},

```

```

{
    "patternNumber": 14,
    "name": "Bad Visibility",
    "description": "Using low contrast, light colors, or
small fonts to make privacy-protective options less visible.",
    "typicalInterfaceLocation": [
        "Cookie banners",
        "Registration process"
    ],
    "observableIndications": [
        "Check whether privacy-protective options (e.g.,
reject, opt-out) are less visible than acceptance options",
        "Identify whether low contrast colors, small fonts,
or faded styling are used for privacy-protective controls",
        "Assess whether the interface visually prioritizes
accepting options while de-emphasizing alternatives such as
reject or manage settings"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [

```

```

        "Presence of privacy-protective options (e.g.,
reject, opt-out) as standard elements but without structural
emphasis",
        "Use of generic elements (e.g., <a>, <span>)
instead of prominent buttons for privacy-protective actions",
        "Privacy-protective controls are present but not
structurally prioritized"
    ],
    "codeExamples": [
        "<button class=\"accept-btn\">Accept
all</button>",
        "<a class=\"reject-link\">Reject</a>"
    ]
},
"cssLayout": {
    "description": [
        "Privacy-protective options are styled with low
contrast (e.g., light colors, faded appearance)",
        "Smaller font size compared to primary actions",
        "Less prominent positioning (e.g., bottom
placement or inline text)"
    ],
    "codeExamples": [
        ".reject-link { color: #aaa; font-size: 12px;
}",
        ".accept-btn { color: white; background-color:
blue; font-size: 16px; }"
    ]
},
"javascriptBehavior": {
    "description": [
        "No direct behavioral restriction, but
visibility influences user interaction",
        "Users are more likely to select visually
prominent options due to layout bias",
        "No additional interaction is required, but UI
design nudges toward the visible option"
    ],
    "codeExamples": [
        "acceptBtn.addEventListener(\"click\",
acceptAll);",
        "rejectBtn.addEventListener(\"click\",
rejectAll);"
    ]
}
},
"gdprMapping": [
    "Article 12(1) - information must be easily
accessible and clear; however, privacy-protective options are
visually de-emphasized using low contrast, small fonts, or
poor visibility.",
    "Article 5(1)(a) - processing must be fair and
transparent; however, visual design reduces the visibility of
privacy choices."
]
}

```

```

    ],
    "prevalence": {
        "count": 15,
        "total": 217,
        "percentage": 6.91
    },
    "keywords": [
        "low contrast",
        "small text",
        "faded",
        "less visible",
        "hard to see",
        "hidden option",
        "secondary option",
        "de-emphasized",
        "not prominent",
        "light grey",
        "grey text"
    ]
},

```

```

{
    "patternNumber": 15,
    "name": "False necessity",
    "description": "Describing privacy-invasive features
as necessary in order to mislead the data subject and distract
from their negative implications.",
    "typicalInterfaceLocation": [
        "Cookie banners",
        "Registration process"
    ],
    "observableIndications": [
        "Check whether optional features (e.g., advertising,
personalization, passkey sign-in) are presented as mandatory
or default choices",
        "Identify whether the stated purpose of data
processing (e.g., \"service improvement\") masks its actual
function (e.g., advertising or tracking)"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Presence of consent or information text
describing optional data processing as necessary or required",
                "Use of wording implying necessity (e.g.,
\"required\", \"needed\", \"essential\") for non-essential
features",
                "Lack of clear distinction between necessary and
optional data processing"
            ],
            "codeExamples": [
                "<p>Personalized advertising is necessary to
support our service.</p>"
            ]
        }
    }
}

```

```

    },
    "cssLayout": {
      "description": [
        "Statements implying necessity are placed prominently within the main consent message",
        "No visual distinction between necessary and optional data processing categories",
        "Text framing makes all processing appear equally important"
      ],
      "codeExamples": [
        ".consent-text { font-weight: normal; color: #333; }"
      ]
    },
    "javascriptBehavior": {
      "description": [
        "Users can proceed by accepting the presented 'necessary' option without clear alternative paths",
        "Optional data processing is treated similarly to required functionality in the interface flow",
        "No explicit distinction in behavior between essential and non-essential data processing"
      ],
      "codeExamples": [
        "if (userAccepted) { enableAds(); enableTracking(); }"
      ]
    },
    "gdprMapping": [
      "Article 12(1) - information must be easily accessible and clear; however, optional data processing is presented as necessary, misleading the user.",
      "Article 5(1)(a) - processing must be fair and transparent; however, the interface falsely frames non-essential processing as required."
    ],
    "prevalence": {
      "count": 5,
      "total": 217,
      "percentage": 2.30
    },
    "keywords": [
      "necessary to use the service",
      "required to use the service",
      "required to access",
      "needed to continue",
      "must enable tracking",
      "must enable personalized advertising",
      "requires enabling",
      "required for full access",
      "necessary for full access"
    ]
  }

```

```

    ],
    },
  ],
  {
    "patternNumber": 16,
    "name": "Forced registration",
    "description": "Tricking the user into believing that registration is necessary in order to access a service, even when it is not required.",
    "typicalInterfaceLocation": [
      "Initial website access (pop-up or login gate)"
    ],
    "observableIndications": [
      "Identify whether registration is framed as necessary even when the service could be used without creating an account"
    ],
    "technicalIndicators": {
      "domHtml": {
        "description": [
          "Presence of login or registration forms as a prerequisite to access content or features",
          "Absence of alternative access options (e.g., guest access, skip login)",
          "Core content or functionality placed behind authentication elements"
        ],
        "codeExamples": [
          "<form id=\"login-form\"><input type=\"email\"><input type=\"password\"><button>Sign up</button></form>"
        ]
      },
      "cssLayout": {
        "description": [
          "Login or registration interface displayed as the primary or only visible screen",
          "Main content is visually hidden or inaccessible behind the login interface",
          "No visible option to bypass or skip registration"
        ],
        "codeExamples": [
          ".login-screen { position: fixed; width: 100%; height: 100%; }"
        ]
      },
      "javascriptBehavior": {
        "description": [
          "Access to content is restricted until the user logs in or registers",
          "No fallback functionality is provided without authentication",
        ]
      }
    }
  }
]

```

```

        "Navigation or interaction is blocked until
registration is completed"
    ],
    "codeExamples": [
        "if (!userLoggedIn) { showLoginScreen(); }"
    ]
}
},
"gdprMapping": [
    "Article 7(4) - consent must be freely given and not
based on processing that is falsely presented as necessary;
however, the interface frames non-essential data processing as
required for the service.",
    "Article 5(1)(a) - processing must be fair and
transparent; however, the interface presents privacy-invasive
features as necessary while downplaying their implications."
],
"prevalence": {
    "count": 1,
    "total": 217,
    "percentage": 0.46
},
"keywords": [
    "must create an account",
    "must create an account to continue",
    "sign up to continue",
    "sign in to continue",
    "required to access",
    "register to continue",
    "registration required",
    "must create an account to access",
    "sign in required",
    "login required to continue"
]
},

```

```

{
    "patternNumber": 17,
    "name": "Nagging",
    "description": "Repeatedly asking the user to accept
or enable something after they have already dismissed or
postponed it, such as selecting \"Not now\" and being asked
again later.",
    "typicalInterfaceLocation": [
        "Home page pop-ups"
    ],
    "observableIndications": [
        "Check whether selecting options like \"Not now\" or
dismissing the prompt does not prevent it from appearing again
later",
        "Assess whether the interface does not provide a
clear or permanent opt-out option for the feature (e.g., no
\"Do not show again\" or equivalent setting)",
    ]
}

```

```

        "Identify whether the prompt continues to appear
despite no explicit user interest or interaction with the
feature"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Presence of recurring prompt elements for the
same request (e.g., notification or signup banner/modal)",
                "Dismissal options such as \"Not now\" are
provided, but no permanent opt-out control is visible",
                "The same prompt structure reappears across
sessions or pages"
            ],
            "codeExamples": [
                "<div class=\"notification-
prompt\"><button>Yes</button><button>Not now</button></div>"
            ]
        },
        "cssLayout": {
            "description": [
                "Prompt appears repeatedly in a prominent
location (e.g., centered modal or top banner)",
                "The same banner or modal styling is reused
after dismissal",
                "No visible \"Do not show again\" or permanent
opt-out option is emphasized"
            ],
            "codeExamples": [
                ".prompt-banner { position: fixed; top: 0;
width: 100%; }"
            ]
        },
        "javascriptBehavior": {
            "description": [
                "Prompt reappears after the user dismisses or
rejects it",
                "Dismissal only hides the prompt temporarily
rather than permanently disabling it",
                "The interface triggers the same request again
after navigation, delay, or future sessions"
            ],
            "codeExamples": [
                "notNowBtn.addEventListener(\"click\", () => {
hidePromptTemporarily(); });"
            ]
        }
    },
    "gdprMapping": [
        "Article 7(4) - consent must be freely given;
however, repeated prompts after refusal pressure the user into
accepting data processing.",
    ]
}

```

```
        "Article 5(1)(a) - processing must be fair; however,
the interface repeatedly asks for consent despite prior
rejection."
```

```
    ],
    "prevalence": {
        "count": 7,
        "total": 217,
        "percentage": 3.23
    },
    "keywords": [
        "not now",
        "maybe later",
        "remind me later",
        "show again",
        "later"
    ]
},
```

```
{
    "patternNumber": 18,
    "name": "Continuous Prompting",
    "description": "Where users are persistently requested
data or authorizations for new users of their personal data.
The constant interruptions can lead to user fatigue , causing
them to relent and provide more personal information or accept
data uses they might otherwise reject.",
    "typicalInterfaceLocation": [
        "Across the entire website"
    ],
    "observableIndications": [
        "Check whether the same request (e.g., "Start free
trial", permission request, upgrade prompt) appears repeatedly
during navigation"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Presence of persistent call-to-action elements
requesting user action (e.g., trial, data sharing,
permissions)",
                "Action prompts embedded within the main
interface rather than isolated in a single interaction",
                "Reusable UI components (e.g., buttons, banners)
repeatedly encouraging the same action"
            ],
            "codeExamples": [
                "<button aria-label=\"Start your free
trial\">Start your free trial</button>"
            ]
        },
        "cssLayout": {
            "description": [
                "Call-to-action elements prominently positioned
within the interface (e.g., top banner, central button)",
```

```

        "Repeated visual emphasis on the same action
across different interface sections",
        "Persistent UI components that remain visible
during navigation"
    ],
    "codeExamples": [
        ".cta-button { position: sticky; top: 0; }"
    ]
},
"javascriptBehavior": {
    "description": [
        "Repeated presentation of prompts across
sessions or navigation",
        "No permanent dismissal option for the prompt",
        "User continues to encounter the same request
over time"
    ],
    "codeExamples": [
        "if (!userStartedTrial) { showCTA(); }"
    ]
},
"gdprMapping": [
    "Article 7(4) - consent must be freely given;
however, continuous prompting and repeated requests create
user fatigue and influence the decision.",
    "Article 5(1)(a) - processing must be fair; however,
repeated interruptions pressure users into accepting data
processing."
],
"prevalence": {
    "count": 1,
    "total": 217,
    "percentage": 0.46
},
"keywords": [
    "start your free trial",
    "upgrade now",
    "enable recommendations",
    "allow notifications",
    "persistent prompt",
    "repeated request"
]
},

```

```

{
    "patternNumber": 19,
    "name": "Conflicting Information",
    "description": "Presenting contradictory information
within the interface, leading to confusion and inaction, often
resulting in users defaulting to pre-set privacy-invasive
options.",
    "typicalInterfaceLocation": [
        "Cookie banners"
    ]
}

```

```

    ],
    "observableIndications": [
      "Check whether the interface presents conflicting
messages about privacy (e.g., claiming strong privacy
protection while encouraging broad data consent)"
    ],
    "technicalIndicators": {
      "domHtml": {
        "description": [
          "Presence of statements that promote privacy
(e.g., \"we respect your privacy\", \"you are in control\")
alongside elements indicating extensive data processing",
          "Contradictory information presented within the
same interface or consent message",
          "Coexistence of reassuring and invasive
descriptions within the same text block"
        ],
        "codeExamples": [
          "<p>We respect your privacy and give you full
control.</p>",
          "<p>We share your data with third-party partners
for advertising.</p>"
        ]
      },
      "cssLayout": {
        "description": [
          "Privacy-reassuring statements are visually
emphasized (e.g., headings, bold text)",
          "Contradictory or invasive information is placed
in less prominent sections (e.g., smaller text, lower
position)",
          "Layout separates positive messaging from
detailed data practices"
        ],
        "codeExamples": [
          ".highlight { font-weight: bold; }",
          ".details { font-size: 12px; color: #666; }"
        ]
      },
      "javascriptBehavior": {
        "description": [
          "Default settings or actions contradict the
reassuring information presented",
          "Interface behavior does not align with the
claims made in the UI text",
          "Users are nudged toward data sharing despite
claims of control"
        ],
        "codeExamples": [
          "if (userAccepted) { enableTracking();
shareWithPartners(); }"
        ]
      }
    },
  },

```

```

      "gdprMapping": [
        "Article 5(1)(a) - personal data must be processed
in a fair and transparent manner; however, the interface
presents contradictory information that misleads users.",
        "Article 12(1) - information must be clear and
intelligible; however, conflicting messages create confusion
about data processing."
      ],
      "prevalence": {
        "count": 1,
        "total": 217,
        "percentage": 0.46
      },
      "keywords": [
        "we respect your privacy",
        "you are in control",
        "privacy matters",
        "share with partners",
        "personalized advertising",
        "tracking"
      ]
    },
  },

```

```

{
  "patternNumber": 20,
  "name": "Friend Spam",
  "description": "Manipulative extraction of information
about other users.",
  "typicalInterfaceLocation": [],
  "observableIndications": [],
  "technicalIndicators": {
    "domHtml": {
      "description": [],
      "codeExamples": []
    },
    "cssLayout": {
      "description": [],
      "codeExamples": []
    },
    "javascriptBehavior": {
      "description": [],
      "codeExamples": []
    }
  },
  "gdprMapping": [
    "Article 5(1)(c) - personal data must be limited to
what is necessary; however, the interface collects personal
data about other individuals that is not required for the
service.",
    "Article 5(1)(a) - processing must be fair and
transparent; however, data about third parties is collected
without their awareness."
  ],
  "prevalence": {

```

```

        "count": 0,
        "total": 217,
        "percentage": 0.0
    },
    "keywords": []
},

```

```

{
    "patternNumber": 21,
    "name": "Language Discontinuity",
    "description": "Despite the service being offered in the official language(s) of the country where users reside, data protection information is not provided in those languages, preventing users from fully understanding how their personal data is processed or how to exercise their rights.",
    "typicalInterfaceLocation": [],
    "observableIndications": [],
    "technicalIndicators": {
        "domHtml": {
            "description": [],
            "codeExamples": []
        },
        "cssLayout": {
            "description": [],
            "codeExamples": []
        },
        "javascriptBehavior": {
            "description": [],
            "codeExamples": []
        }
    },
    "gdprMapping": [
        "Article 12(1) - information must be provided in an intelligible and clear and plain language; however, privacy-related information is not provided in the user's language, limiting understanding.",
        "Article 5(1)(a) - processing must be transparent; however, users cannot fully understand how their data is processed due to language barriers."
    ],
    "prevalence": {
        "count": 0,
        "total": 217,
        "percentage": 0.0
    },
    "keywords": []
},

```

```

{
    "patternNumber": 22,
    "name": "Immortal Accounts",
    "description": "Account and consumer information cannot be permanently deleted.",
    "typicalInterfaceLocation": [

```

```

        "Delete account process"
    ],
    "observableIndications": [
        "Check whether there is no option to permanently
delete the account within the interface",
        "Identify whether the platform offers only
deactivation instead of full account deletion"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Absence of a \"Delete account\" option in account
settings",
                "Presence of only \"Deactivate\", \"Disable\", or
\"Close account\" options",
                "Lack of interface elements enabling permanent
deletion of user data"
            ],
            "codeExamples": [
                "<button>Deactivate account</button>"
            ]
        },
        "cssLayout": {
            "description": [
                "Deactivation options are prominently displayed,
while deletion is not present",
                "No visible controls related to permanent data
erasure",
                "Interface suggests account closure without
clearly offering deletion"
            ],
            "codeExamples": [
                ".deactivate-btn { background-color: gray; }"
            ]
        },
        "javascriptBehavior": {
            "description": [
                "Account closure does not trigger deletion of
stored personal data",
                "Additional external steps are required to
request deletion (e.g., email support)",
                "The system retains user data after account
deactivation"
            ],
            "codeExamples": [
                "function deactivateAccount() {
disableAccount(); /* data still stored */ }"
            ]
        }
    },
    "gdprMapping": [
        "Article 17 - the data subject has the right to
obtain erasure of personal data; however, accounts or
associated data cannot be fully deleted.",
    ]
}

```

```
        "Article 12(2) - the controller shall facilitate the exercise of data subject rights; however, deletion is not possible or not accessible."
```

```
    ],  
    "prevalence": {  
        "count": 4,  
        "total": 217,  
        "percentage": 1.84  
    },  
    "keywords": [  
        "deactivate account",  
        "disable account",  
        "close account",  
        "no delete option",  
        "cannot delete"  
    ]  
},
```

```
{  
    "patternNumber": 23,  
    "name": "Privacy invasive defaults",  
    "description": "Privacy-invasive defaults where privacy-related settings are configured to share or expose personal data by default.",  
    "typicalInterfaceLocation": [  
        "Account information"  
    ],  
    "observableIndications": [  
        "Check whether privacy-related settings (e.g., profile visibility, activity sharing) are set to public by default"  
    ],  
    "technicalIndicators": {  
        "domHtml": {  
            "description": [  
                "Presence of privacy-related settings with public or sharing-enabled default values",  
                "Toggles or checkboxes for visibility, sharing, or personalization enabled in the initial state",  
                "No explicit opt-in is required before personal data becomes visible or shared"  
            ],  
            "codeExamples": [  
                "<input type=\"checkbox\" id=\"publicProfile\" checked>",  
                "<input type=\"checkbox\" id=\"shareActivity\" checked>"  
            ]  
        },  
        "cssLayout": {  
            "description": [  
                "Public or sharing-enabled options are visually shown as active by default",  
                ]  
        }  
    }  
}
```

```

        "Default visible state is indicated through
active toggles, checked boxes, or selected buttons",
        "No equal visual emphasis is given to more
privacy-protective alternatives"
    ],
    "codeExamples": [
        "input[type=checkbox]:checked + label::before {
background-color: blue; }"
    ]
},
"javascriptBehavior": {
    "description": [
        "Personal data becomes visible or shareable
unless the user manually changes the default settings",
        "Public-facing or data-sharing behavior is
enabled automatically on account creation or first use",
        "The system assumes exposure unless the user
opts out"
    ],
    "codeExamples": [
        "if
(document.getElementById(\"publicProfile\").checked) {
makeProfilePublic(); }"
    ]
},
"gdprMapping": [
    "Article 25(2) - by default, only personal data
which are necessary should be processed, and data should not
be made accessible without user intervention; however,
personal data is publicly visible or shared by default.",
    "Article 5(1)(a) - processing must be fair and
transparent; however, users are exposed to data sharing
without explicit action."
],
"prevalence": {
    "count": 7,
    "total": 217,
    "percentage": 3.23
},
"keywords": [
    "public profile",
    "make my profile public",
    "share my activity",
    "share activity",
    "profile visibility",
    "activity visibility",
    "public visibility",
    "visible to everyone",
    "show my activity",
    "allow others to see my profile"
]
]

```

```

    },
  {
    "patternNumber": 24,
    "name": "Too many options method",
    "description": "Overwhelming users with a large number of options, leading to decision paralysis or accidental oversight of important privacy settings.",
    "typicalInterfaceLocation": [
      "Cookie banners",
      "Pop-ups about personal data"
    ],
    "observableIndications": [
      "Check whether the consent interface presents a very large number of options (e.g., hundreds of partners or multiple processing purposes)",
      "Identify whether the volume of information (e.g., long lists of vendors, purposes) makes it difficult to review or understand choices",
      "Assess whether users are required to navigate through extensive lists to manage or customize consent",
      "Identify whether the overwhelming number of options encourages users to accept all instead of reviewing individual settings"
    ],
    "technicalIndicators": {
      "domHtml": {
        "description": [
          "Presence of large lists of third-party partners or vendors in the consent interface",
          "Multiple data processing purposes presented simultaneously",
          "Extensive number of checkboxes or toggles related to different processing activities"
        ],
        "codeExamples": [
          "<div class=\"partners-list\"><p>We work with 300+ partners</p></div>",
          "<div class=\"purposes\"><label><input type=\"checkbox\"> Analytics</label><label><input type=\"checkbox\"> Advertising</label><label><input type=\"checkbox\"> Personalization</label></div>"
        ]
      },
      "cssLayout": {
        "description": [
          "Long scrollable lists of partners or purposes within the consent interface",
          "Dense layout with many controls displayed at once",
          "Lack of simplification or grouping that would support easy decision-making"
        ],
        "codeExamples": [

```

```

        ".partners-list { max-height: 300px; overflow-y:
scroll; }"
    ],
    },
    "javascriptBehavior": {
        "description": [
            "Interface allows granular control but requires
extensive interaction to configure preferences",
            "No simplified or user-friendly way to manage
consent without navigating many options",
            "High interaction cost encourages users to
select default options (e.g., "Accept all")"
        ],
        "codeExamples": [
            "partners.forEach(p => renderPartnerToggle(p));"
        ]
    },
    },
    "gdprMapping": [
        "Article 12(1) - information must be concise and
intelligible; however, the interface presents excessive and
complex options that overwhelm users and hinder
understanding.",
        "Article 7(2) - consent must be provided in an
intelligible form; however, the volume of options makes
meaningful consent difficult."
    ],
    "prevalence": {
        "count": 15,
        "total": 217,
        "percentage": 6.91
    },
    "keywords": [
        "partners",
        "vendors",
        "purposes",
        "analytics",
        "advertising",
        "personalization",
        "300+ partners"
    ]
},

```

```

{
    "patternNumber": 25,
    "name": "Account Registration",
    "description": "No explicit consent checkbox is
provided during registration, and agreement is implied through
account creation.",
    "typicalInterfaceLocation": [
        "Registration process"
    ],
    "observableIndications": [

```

```

        "Check whether consent is presented as small, low-
        visibility text within the registration form (e.g., below the
        sign-up button or in fine print)",
        "Identify whether no explicit consent checkbox is
        provided and agreement is implied by completing registration"
    ],
    "technicalIndicators": {
        "domHtml": {
            "description": [
                "Absence of a consent checkbox in the
                registration form",
                "Presence of agreement text indicating that
                consent is implied through account creation",
                "Links to terms and privacy policy provided
                without requiring explicit interaction"
            ],
            "codeExamples": [
                "<div>By joining, you agree to our Terms and
                Privacy Policy.<a href=\"/terms\"></a><a
                href=\"/privacy\"></a></div>"
            ]
        },
        "cssLayout": {
            "description": [
                "Consent text is displayed in small or secondary
                text near the registration button",
                "No interactive element (e.g., checkbox) is
                provided for explicit consent",
                "Terms and privacy links are visually de-
                emphasized compared to the main sign-up action"
            ],
            "codeExamples": [
                ".terms-text { font-size: 12px; color: #777; }"
            ]
        },
        "javascriptBehavior": {
            "description": [
                "Account creation proceeds without requiring
                explicit consent action",
                "Submission of the form is treated as implicit
                agreement to terms and privacy policy",
                "No validation step enforces active consent
                before registration"
            ],
            "codeExamples": [
                "form.addEventListener(\"submit\", () => {
                createAccount(); });"
            ]
        },
        "gdprMapping": [
            "Article 7(1) - consent requires a clear affirmative
            action; however, agreement is implied without any explicit
            user action.",

```

```
        "Article 4(11) - consent must be a clear affirmative  
action; however, no such action is required during  
registration."
```

```
    ],  
    "prevalence": {  
        "count": 29,  
        "total": 217,  
        "percentage": 13.36  
    },  
    "keywords": [  
        "by creating an account",  
        "by signing up",  
        "by joining",  
        "you agree to our terms",  
        "by continuing, you agree",  
        "by registering, you agree",  
        "creating an account means you agree"  
    ]
```