

# Comparing Nudges and Deceptive Patterns at a Technical Level

Mathias Schlolaut<sup>1,\*†</sup>, Olga Kieselmann<sup>1†</sup> and Arno Wacker<sup>1†</sup>

<sup>1</sup>University of the Bundeswehr Munich, Germany

## Abstract

Nowadays, two concepts are widely used to influence users' behavior on websites. These are deceptive patterns and nudges. In the literature, the two concepts are distinguished according to their goals and effects. While deceptive patterns are considered as manipulation of users, nudges have a more positive connotation – they are meant to motivate users to make better decisions. However, looking at these concepts from a technical perspective, the question arises whether they also differ in their realization. Is it possible to automatically differentiate between them while crawling a web page for deceptive patterns? To answer this question, we developed a methodology that we present and apply in this paper. Furthermore, we show that there is no need to distinguish between the two concepts, because they are implemented using the same techniques.

## Keywords

dark patterns, deceptive patterns, nudging

## 1. Introduction

Our research focus is to automatically identify if website providers use deceptive patterns on their websites. Thereby, one of our goals is to observe and analyze changes of cookie banners in terms of deceptive patterns over time. Consequently, we could use the analysis results, e.g., to determine whether legal regulations have an impact on cookie banners in the EU or worldwide and for other topics relevant with regard to privacy as deceptive patterns are more and more used to undermine the users defense. To achieve our goal, the logical start would be to capture cookie banners and, then, identify if they use deceptive patterns. However, to identify deceptive patterns, we must first understand what a deceptive pattern is. Only then we can choose appropriate technical tools to detect them. Hence, our *first research question* is not only to understand what a deceptive pattern is, but also to systemize the types of deceptive patterns and to determine whether each type is technically detectable. Furthermore, website providers could also use nudges. At first impression, nudges are a different concept than the deceptive patterns. However, if you try to distinguish between the two concepts from a crawler's point of view, uncertainty arises as to how exactly you should differentiate between them technically. Consequently, our *second research question* is about the implementation of deceptive patterns and nudges in websites. Do we have to differentiate between deceptive patterns and nudges if crawling for them?

To find answers, we developed and applied a methodology for comparing deceptive patterns and nudges. Our results show that there is no difference between deceptive patterns and nudges from the technical point of view. This methodology also applies to upcoming types of deceptive patterns or nudges. Moreover, we provide an overview of currently detectable deceptive patterns and nudges from the perspective of a crawler.

The rest of the paper is organized as follows: In Section 2, we present our system model. Then, in Section 3 and 4, we define the terms *deceptive pattern* and *nudging* to understand the concepts behind them. We describe our methodology for comparing those concepts in Section 5. To decide whether

---

*Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices Workshop at CHI conference on Human Factors in Computing Systems, May 12, 2024, Honolulu, HI (Hybrid Workshop)*

\*Corresponding author.

†These authors contributed equally.

✉ mathias.schlolaut@unibw.de (M. Schlolaut); olga.kieselmann@unibw.de (O. Kieselmann); arno.wacker@unibw.de (A. Wacker)

ORCID 0009-0007-0892-8929 (M. Schlolaut); 0009-0006-9342-0873 (O. Kieselmann); 0009-0009-3293-6624 (A. Wacker)



© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

both concepts are the same from a technical point of view, we apply our methodology and analyze the results in Section 6. In Section 7, we discuss related work. Finally, we conclude our paper with a brief summary and provide an outlook in Section 8.

## 2. System Model

Our system is based on the idea to use a crawler to examine websites in the context of deceptive patterns. Such a *crawler* could be a framework like OpenWPM (Open Web Privacy Measurements). The purpose of this framework is to assist researchers and developers in analyzing privacy-related aspects of web browsing and online tracking [1].

Our crawler mimics a user visiting a *webpage*, analyzing its source code to extract visible parts, ensuring the data reflects what a user sees for accurate identification of deceptive patterns. We consider only the types of *deceptive patterns* whose capturing is technically feasible. Hence, deceptive patterns that aim to trigger certain reaction in users through the content of images or texts are out of our scope.

In general, the providers of websites have specific goals. According to these goals, the web designers create user interface designs to guide people's behavior in digital choice environments [2]. We refer to such user interface designs from now on just as *design*. Furthermore, we use the term *technique* to refer to technical implementations of these designs. For instance, a popup might utilize HTML for structure, Javascript for loading, and CSS for styling.

In summary, the main components of our system are web pages, the techniques used on the web pages, and a crawler that analyses the designs of the web pages. We focus on the designs that are shown to users and are technically identifiable. Thereby, legal and ethical aspects are not part of this work, as they are not relevant to decide if it is technical feasible to identify such designs or not.

## 3. Deceptive Patterns

As Harry Brignull coined the term *dark pattern* and later replaced it with the term *deceptive patterns*, we use his definition. In [3], he identifies deceptive patterns as manipulations on websites and apps causing unintended actions, like unintended purchases or sign-ups. These patterns are unique from regular design patterns as they manipulate human decision-making weaknesses to prompt user action [4].

In [5], Luguri and Strahilevitz show the effectiveness of deceptive patterns. They examined how variations in user interface design, including *mild dark patterns* and additional click-through screens, significantly increased acceptance of a questionable data protection plan among different groups.

Besides the term *deceptive pattern*, there are other terms with the same or very similar meaning. These terms are: dark patterns, aggressive dark patterns [5], dark nudging [6], deceptive content [7], deceptive dark patterns [8], deceptive pattern [3], digital dark nudge [9], mild dark patterns [5], sludge [10]. We consider these terms as synonyms and use only the term *deceptive patterns* in the rest of the paper.

## 4. Nudging

Unlike deceptive patterns, there is no standard and precise definition of the term *nudge*. We adopt Richard Thaler and Cass Sunstein's interpretation from the updated version of their book, aligning with Meske et al. [11]. However, we reference the updated edition [10]. Accordingly, Thaler and Sunstein [10, p. 6-8] describe nudges as choices left open, unobstructed, or unburdened, emphasizing freedom of choice. They further detail that nudges should guide people towards improving their lives, alter behavior predictably without limiting options or altering economic incentives significantly, and be easy and inexpensive to avoid.

Similar to deceptive patterns, there are various terms for nudges that refer to more or less the same meaning. In the following, we list some examples: bright pattern ("privacy-friendly design nudges") [12], default nudges [13], digital nudging [2], green nudging [14], nudging elements [11], nudging

mechanisms [15], nudging techniques [16], privacy nudges[13], self-nudging[17], soft paternalistic interventions[18]. We treat these terms as synonyms and use the term *nudges* in the rest of the paper.

## 5. Methodology

To address our research questions outlined in Section 1, we systematically explore the similarities and differences between deceptive patterns and nudges using a methodology we developed. This section details each step of our approach.

**Step 1. Literature Review** We start with the literature review. When searching for relevant papers, we use the following keywords or their combination: dark patterns, deceptive patterns, comparing, comparison, vs, nudges, and nudging. To ensure the relevance of the papers, we set specific criteria:

1. It was published after 2008. The reason for this is that the term *nudge* was only coined in 2008. In turn, the term *dark pattern* was introduced in 2010.
2. It contains an explanation of specific designs.
3. The authors consider either deceptive patterns or nudges.
4. The authors compare deceptive patterns and nudges.

We divide the literature review into two parts: the search for papers on deceptive patterns, and the search for papers on nudges. To organize the review results, we use a separate table for each part. These tables consist of two columns: In the first column, we list the name of a design. In the second column, we place a short description of the corresponding design. With a design, we mean either a deceptive pattern or a nudge.

This step serves to get an overview of existing types of deceptive patterns and nudges exist. It results in two tables: the one contains the identified deceptive patterns, the other the nudges.

**Step 2. Implementation Review** Based on the results from the previous step, we examine which technique exist to implement deceptive patterns or nudges in web applications. For this, we analyze the current literature and assess the identified methods for relevance to our project. We consider a technique as relevant if it fulfills the following two requirements:

1. It is applicable to implement a deceptive pattern or a nudge.
2. It can be detected automatically, e.g., with the help of a crawler.

This step is split into two parts: one focusing on deceptive patterns and the other on nudges. Using the tables from Step 1, we identify applicable techniques for each design. To organize the results, we add another column. Thus, we get a table with three columns: the first for the designs, the second for the description, and the third for the technique. Per row, we get for each design an information with which technique it can be implemented.

This step serves to gather techniques that are available to implement the designs collected in Step 1. It results in two extended tables: the one gives an overview of relevant techniques available for deceptive patterns, the other for the nudges.

**Step 3. Filtering** Due to our requirements in Step 2, it is possible that some designs were not extended with a technique. Therefore, in this step, we analyze the two resulting tables from Step 2. If there is an item without a technique in the corresponding column, we delete this row.

The aim of this step is to get an overview of automatically detectable designs. This step results in the two cleaned tables: the one gives an overview of relevant deceptive patterns (Table 1), the other for the nudges (Table 2). In the following, we consider only the designs that remain after this step.

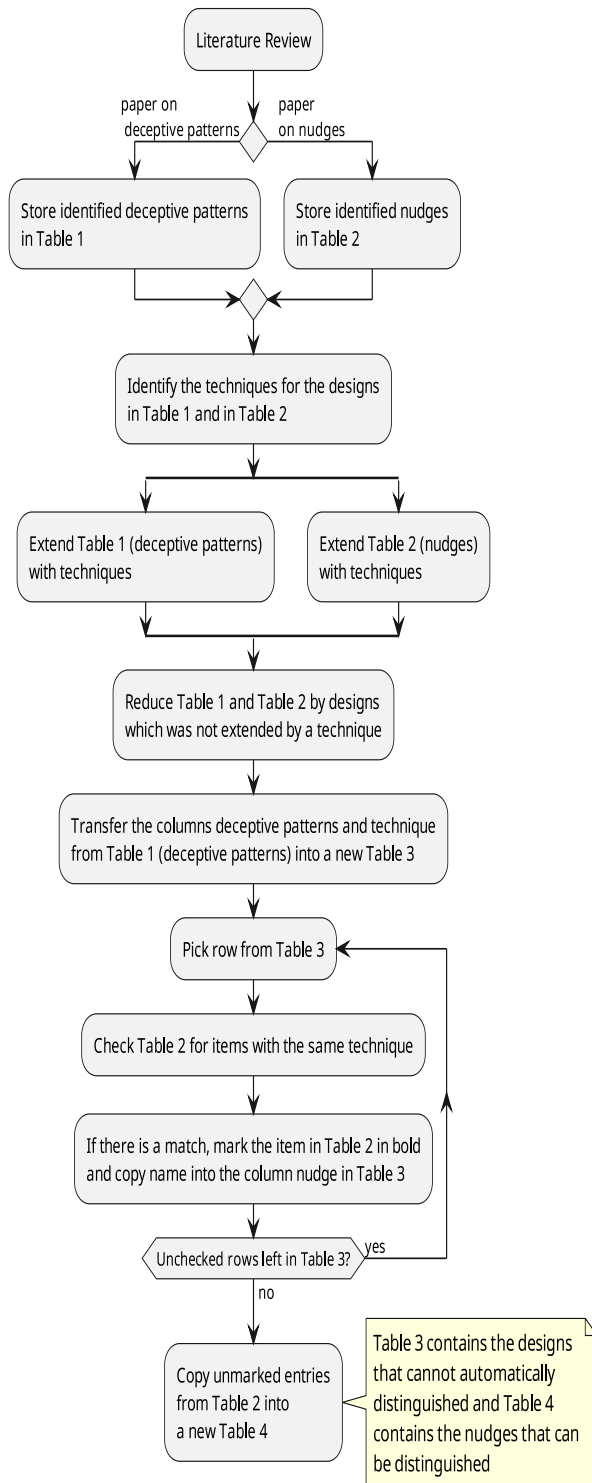


Figure 1: Activity Diagram representing our Methodology

only a snapshot. Technology is continuously evolving, and new insights into behavioral psychology are possible. Thus, innovative techniques may soon be available to implement old or novel nudges or deceptive patterns. However, with our method, the results from previous iterations can be extended by new elements to analyze the current situation.

**Step 4. Comparison** In this step, we compare the deceptive patterns and nudges to each other. For that, we analyze the two tables from Step 3. To store the results of our comparison, we prepare another table (Table 3) with the following columns: *Deceptive Pattern*, *Nudge* and *Technique*. Next, we transfer the columns *Deceptive Pattern* and *Technique* from Table 1 to Table 3. For the following analysis, we can ignore Table 1, as the relevant information is now available in Table 3.

Next, for each row in Table 3, we examine the column *Technique* in the table with nudges (Table 2) to check if there is an item that uses the same technique. Whenever we find a match in Table 2, we mark the corresponding nudge name in bold indicating that we have already considered it. Additionally, we put the name of this nudge in column *Nudge* in the current row in Table 3. This step is completed after we have considered all rows in Table 3.

With this step, we aim to identify if there are deceptive patterns and nudges that use the same techniques. The result is an overview of designs that might have different names, but are implemented with the same techniques.

**Step 5. Identifying Differences** In this step, we examine Table 2 and focus on the entries that are not marked in bold. They were not marked in the previous step, because none of the examined deceptive patterns uses the same technique. Therefore, we consider the corresponding nudges as distinguishable by the technique used. For a better overview, we copy the not marked rows into a new table (Table 4).

We complete our comparison of deceptive patterns and nudges when we make a decision about each design we collected in Step 1. In the end, we have two tables: Table 3 with designs that we cannot automatically distinguish, and Table 4 with nudges that we can distinguish from deceptive patterns by the technique. Based on the results after Step 5, we should be able to answer our research questions. Our methodology is represented as a diagram in Figure 1.

It must be kept in mind that the results are

## 6. Analysis of Differences

In this section, we apply our methodology (see Section 5) to determine if, and if so, what techniques we can use in order to distinguish deceptive patterns from nudges.

**Step 1. Literature Review** In this step, we identified that Mathur et al. [19] published a literature review on deceptive patterns. In this paper, the authors organize the deceptive patterns by paper. As a result, they provide a list of deceptive patterns for each paper. Based on our previous research, we can confirm that they list all deceptive patterns that we know. Additionally, they provide a short description for each listed deceptive pattern. Hence, we can use this list for our analysis. We transfer the listed deceptive patterns with their descriptions in a table (Table 1). However, some deceptive patterns are listed in several groups. Thereby, they have different names, but a very close description. For example, there is a deceptive pattern ‘Bait & Switch’ with the description “You set out to do one thing, but a different, undesirable thing happens instead.” from [3]. A very similar deceptive pattern with the name ‘Bait & Change’. In [20], the authors describe it as “A setting or a choice made by the individual produces a different result than desired.”[20]. In such cases, we select only one version and omit others. Additionally, we group the same deceptive patterns together, for example ‘Address Book Leeching’ and ‘Social Pyramid Schemes’, as they both are based on a social factor to obtain contacts or contact lists.

There is a similar work on nudges. Jesse et al. [21] conducted a systematic literature review on nudges and provide a well-structured list of existing nudges. We transfer these nudges and their descriptions in the second table (Table 2).

**Step 2. Implementation Review** No existing work catalogs techniques for implementing deceptive patterns or nudges. Therefore, we analyzed web design techniques meeting our criteria: applicability to deceptive patterns or nudges and automatic detectability.

In the following, we list the techniques that fulfill our requirements, and give an example of what they can be used for: *audio* (a sound to create attention), *color* (aggressive colors to increase the salience), *fonts* (text differs from the rest of the text/website), *highlighting* (changes the background color, putting a frame around text), *images* (catching the attention of the user), *mandatory field entries* (field in a form that need to be filled out to proceed), *popup* (block the website completely, or partially, to urge the user into interaction with the popup), *preselected checkboxes* (opt-out, preselected options which the user have to deactivate), *progress bar* (to show the user how close or far he is to the goal).

Another technique which we consider as detectable, but is not implemented with a single technique is *nested path*, where the user have to click through, e.g., menus. The last technique that we consider relevant is *wording*. It is not really a technique in our definition, but it is an important component of many deceptive patterns and nudges, e.g., when communicating the behavior of others.

Our focus on basic techniques excludes methods like blinking or rapid color changes, as these are combinations of color and highlighting—techniques already accounted for in our analysis.

Having the list with techniques, we extend Table 1<sup>1</sup> with the column *Technique*. After that, we verify row by row which technique can be used to implement the deceptive pattern in the current line. If we do not find an appropriate technique, this cell remains empty, and we proceed with the next row. We do the same for the table with nudges (Table 2<sup>2</sup>).

**Step 3. Filtering** In this step, we check Table 1, scrutinizing the column *Technique* for empty cells. Empty cells indicate that the corresponding deceptive pattern lacks a technically detectable implementation method. Consequently, we delete rows with empty *Technique* cells. In general, this has affected deceptive patterns that are based on complex ideas and cannot be implemented with basic techniques. For instance, the collective term ‘sneaking’ is too broad in its descriptions as “an attempt to hide, disguise, or delay the divulging of information that has relevance to the user” [25]. We cannot

<sup>1</sup>Due to the size, we show Table 1 only after Step 3.

<sup>2</sup>Due to the size, we show Table 2 only after Step 4.



**Table 1**  
Deceptive Patterns for Webdesigns

Deceptive Pattern	Description	Technique
Address Book Leeching, Social Pyramid Schemes	“A service provider offers users to upload or import their address books to connect with known contacts on that service.” [22]	wording
Attention Grabber	“Attracting attention of a passerby is an exceedingly common strategy used by anyone selling a product or service: the goal is to turn the passerby into a customer.” [23]	audio, color, fonts, highlighting, images, popup
Bad Defaults[22], Default Settings[24] and preselection[25]	“[...] usually manifests as a default choice [...]; however, this choice is often against the user’s interests or may provide unintended consequences.”[26]	preselected checkboxes
Bait and switch	“You set out to do one thing, but a different, undesirable thing happens instead.”[3]	audio, popup
Coercion	“Threatening or mandating the user’s compliance.”[27]	mandatory field entries
Confirmshaming	“The act of guiltling the user into opting into something. The option to decline is worded in such a way as to shame the user into compliance.” [3]	preselected checkboxes, popup, wording
Disguised Ads	“Adverts that are disguised as other kinds of content or navigation, in order to get you to click on them.” [3]	linking
Distraction	“Attracting the user’s attention away from their current task by exploiting perception, particularly preattentive processing.” [27]	audio, color, popup
Ease	“[...] lead users in a certain direction, making the process toward the alternatives a long and arduous process[...].”[24]	nested path
Immortal Accounts	“[...] the service provider prevents the user from doing so by either—unnecessarily complicating the account deletion experience, or by not providing any account deletion option at all.”[22]	absent information, nested path
Interface Interference	“[...] any manipulation of the user interface that privileges specific actions over others, thereby confusing the user or limiting discoverability of important action possibilities [...]”[25]	preselected checkboxes, highlighting, nested path
Interruption	“Interrupting the user’s task flow.” [27]	popup
Misdirection[3][7]	“[...] focuses your attention on one thing in order to distract your attention from another.” [3]	audio, color, fonts, highlighting, images, popup
Obfuscation	“Hiding desired information and interface elements.” [27]	color, fonts, nested path
Privacy Zuckering	“You are tricked into publicly sharing more information about yourself than you really intended to.” [3]	mandatory field entries, progress bar, wording
Scarcity	“ ‘Scarcity’ [...] signal the limited availability or high demand of a product, thus increasing its perceived value and desirability”[7]	highlighting, wording
Social proof	“informing users of others’ behavior and shopping with others”[7]	highlighting, wording

apply a concrete technique to such a description. Further examples of deceptive patterns that we cannot map to a technique are: cuteness of robots, entrapping, two-faced and sneaking. We present the resulting overview of deceptive patterns that we can automatically detect in Table 1.

**Table 2**  
Nudges for Webdesigns

nudging	description	technique
<b>Attracting/ Reducing attention</b>	“A mechanism which tries to draw attention to certain options or information with the use of highlighting.”[21]	color, fonts, highlighting, images, popup, wording
<b>Change financial effort</b>	“Choice architects can intervene with the perception of financial effort. Examples include postponing costs to the future without changing the actual final costs.”[21]	preselected checkboxes, wording
<b>Following the herd (norm)</b>	“As users do not want to stick out, they have a tendency to do what the majority of people does.”[21]	highlighting, wording
<b>Hiding information</b>	“Make undesirable options or information harder to see.”[21]	color, fonts, nested path
<b>Increase salience of attribute</b>	“The act of making an attribute more salient (e.g., weight, price or color)”[21]	color, fonts, highlighting, images
<b>Increase salience of incentives</b>	“Make incentives more salient or visible, so they are more effective and prominent.”[21]	color, fonts, highlighting, images
<b>Limited time window</b>	“When an option is presented as only being available for a certain amount of time it is perceived as more important and scarce.”[21]	highlighting, wording
<b>Loss aversion</b>	“Describes the phenomena of users weighting losses higher than winnings (e.g., the loss of €100 is worse than winning €100)”[21]	wording
<b>Make resources scarce</b>	“Announcing limited availability of an option increases the probability of users committing to choosing it.”[21]	highlighting, wording
<b>Providing Feedback</b>	“Providing users with feedback when they are doing well or making mistakes”[2]	popup, progress bar, wording
<b>Remind of socially desirable concepts</b>	“Influence users by stating the social expectation in a specific situation (e.g., need to vote)”[21]	highlighting, wording
<b>Setting defaults</b>	“Preselecting options by setting default options”[2]	preselected checkboxes
<b>Suggesting alternatives</b>	“Provide the users with alternatives that they might not have considered at this point (e.g., cheaper camera with the same resolution)”[21]	highlighting, popup, wording
<b>Using visuals to deceive</b>	“Through the use of optical illusions the perception and judgment of options is altered, so they appear more salient than they actually are.”[21]	color, fonts, highlighting, images
<b>Using visuals to increase salience</b>	“The salience of information is increased with the use of visual effects (e.g., colors, pictures, signs or fonts)”[21]	color, fonts, highlighting, images
<b>Visible goals</b>	“Make simple performance measures clearly visible so that people can immediately assess their performance against a goal state (e.g., clearly displaying manufacturing output and goals in factories is often, by itself, sufficient to increase productivity).”[28]	color, highlighting, progress bar
<b>Warning</b>	“Warn the users with the help of visuals or other means that emphasize the problem at hand.”[21]	highlighting, popup, wording

Similarly, we proceed with Table 2: we search for empty cells in the column *Technique*, i.e., for nudges that are too broad in their meaning or could not be implemented with the techniques from Step 2. If we find such a nudge, we delete the whole row. Examples for such nudges are: decrease vagueness and ambiguity, providing multiple viewpoints, simplification and understanding mapping. In Table 2, we show the remaining nudges. These are nudges that we can automatically identify.

**Table 3**  
Comparing Deceptive Patterns and Nudges

Deceptive Pattern	Nudge	Technique
Address Book Leeching	Attracting attention, Financial effort, Following the herd, Limited time, Loss aversion, Scarce resources, Feedback, Socially desirable concepts, Alternatives, Warning	wording
Attention Grabber	Attracting attention, Following the herd, Hiding Information, Saliency of attribute, Saliency of incentives, Limited time, Scarce resources, Feedback, Socially desirable concepts, Alternatives, Visuals to deceive, Visuals to increase saliency, Visible goals, Warning	audio, color, fonts, highlighting, images, popup
Default Settings	Financial effort, Defaults	preselect checkboxes
Bait and switch	Attracting attention, Feedback, Alternatives, Warning	audio, popup
Coercion		mandatory field entries
Confirmshaming	Attracting attention, Financial effort, Following the herd, Limited time, Loss aversion, Scarce resources, Feedback, Socially desirable concepts, Defaults, Alternatives, Warning	preselected checkboxes, popup, wording
Disguised Ads		linking
Distraction	Attracting attention, Hiding Information, Saliency of attribute, Saliency of incentives, Feedback, Alternatives, Visuals to deceive, Visuals to increase saliency, Visible goals, Warning	audio, color, popup
Ease		nested path
Immortal Accounts		absent information, nested path
Interface Interference	Attracting attention, Financial effort, Following the herd, Saliency of attribute, Saliency of incentives, Limited time, Scarce resources, Socially desirable concepts, Defaults, Alternatives, Visuals to deceive, Visuals to increase saliency, Visible goals, Warning	preselected checkboxes, highlighting, nested path
Interruption	Attracting attention, Feedback, Alternatives, Warning	popup
Misdirection	Attracting attention, Following the herd, Hiding Information, Saliency of attribute, Saliency of incentives, Limited time, Scarce resources, Feedback, Socially desirable concepts, Alternatives, Visuals to deceive, Visuals to increase saliency, Visible goals, Warning	audio, color, fonts, highlighting, images, popup
Obfuscation	Attracting attention, Hiding Information, Saliency of attribute, Saliency of incentives, Visuals to deceive, Visuals to increase saliency, Visible goals	color, fonts, nested path
Privacy Zuckering	Attracting attention, Financial effort, Following the herd, Limited time, Loss aversion, Scarce resources, Feedback, Socially desirable concepts, Alternatives, Visible goals, Warning	mandatory field entries, progress bar, wording
Scarcity	Attracting attention, Financial effort, Following the herd, Saliency of attribute, Saliency of incentives, Limited time, Loss aversion, Scarce resources, Feedback, Socially desirable concepts, Alternatives, Visuals to deceive, Visuals to increase saliency, Visible goals, Warning	highlighting, wording
Social Proof	Attracting attention, Financial effort, Following the herd, Saliency of attribute, Saliency of incentives, Limited time, Loss aversion, Scarce resources, Feedback, Socially desirable concepts, Alternatives, Visuals to deceive, Visuals to increase saliency, Visible goals, Warning	highlighting, wording

**Step 4. Comparison** In this step, we transfer the *Deceptive Pattern* and *Technique* columns from Table 1 to Table 3. Next, we identify any nudges in Table 2 that utilize the same techniques as the deceptive patterns. Upon finding such matches, we highlight the corresponding nudges in Table 2 in



bold. Then, we put the names of these nudges in the *Nudge* column for the relevant row in Table 3, displaying the findings of our analysis.

**Step 5. Identifying Differences** Having Table 3, we begin to evaluate if we can distinguish nudges from deceptive patterns. If there are some unmarked nudges available in Table 2, we can identify these nudges as distinguishable from deceptive patterns by the techniques they use. However, all nudges are marked in bold, i.e., there is no nudge that we can distinguish from deceptive patterns. In contrast, there are deceptive patterns that do not share techniques with any nudge from Table 2. We identify such deceptive patterns by empty cells in the column *Nudge*. These deceptive patterns are: absent information, audio, nested path, mandatory field entries. Therefore, based on this information, we conclude that it is not technically feasible to distinguish nudges from deceptive patterns. This is because there are no techniques in nudges which are not also used by deceptive patterns. Thus, a crawler cannot discern whether a technique is used by a nudge or by a deceptive pattern.

## 7. Related Work

There are several papers that focus on the study of deceptive patterns or nudges. There are also some papers that address the fact that there is overlap between deceptive pattern and nudges. However, to the very best of our knowledge, there is no work that compares deceptive patterns and nudges systematically and from a technical perspective. In the following, we discuss only those papers that at least mention the differences and similarities between the two concepts.

Narayanan et al. [29] state that deceptive patterns are a result from three decade-long trends: retail (deceptive practices), research and public policy (nudging), and the design community (growth hacking). The authors classify research on nudges as a source of deceptive patterns. Here, nudging refers to the 1970s, when “the heuristics and biases literature of behavioral economics sought to understand irrational decisions and behaviors” [29]. Thus, the authors see a connection between deceptive patterns and nudges, based on the idea that deceptive patterns have evolved from, among other things, nudging. However, they focus only on a few examples and a few designs, and do not go beyond that.

Morrison et al. [30] highlight that dark patterns intersect deceptive techniques, nudging, and social engineering, building on Narayanan et al. [29]. In contrast to our work, they refer to mental models and do not go beyond that point either.

In other papers, the authors do not directly link deceptive patterns and nudges, but do acknowledge their presence. For example, Weinzierl [6] introduces “dark nudging” as a term to bridge deceptive patterns with the behavioral psychology principles underlying nudging. In [5], the authors discuss the blurred lines between persuasion and manipulation, noting the possibility that designers might unknowingly create interfaces with deceptive patterns, highlighting the challenges in differentiating between deceptive patterns and nudges. Jesse and Jannach [21] remark on the difficulty of clearly separating nudging from persuasion, emphasizing that both are aimed at influencing user behavior and decisions. The key distinction they note is whether the influence is beneficial or detrimental to the user.

## 8. Conclusion

We investigated the technical possibility of differentiating nudges from deceptive patterns in web analysis. Our developed methodology showed that, technically, both concepts are indistinguishable, suggesting crawlers may capture both deceptive and non-deceptive patterns alike.

In future work, we will examine what additional features or their combination we can integrate to enable the differentiation. For this, we will first analyze whether and how we can use wording to automatically distinguish between deceptive patterns and nudges.

## References

- [1] S. Englehardt, A. Narayanan, Online tracking: A 1-million-site measurement and analysis, in: *Proceedings of ACM CCS 2016*, 2016, pp. 1388–1401. doi:10.1145/2976749.2978313.
- [2] M. Weinmann, C. Schneider, J. v. Brocke, Digital nudging, *Business & Information Systems Engineering* 58 (2016) 433–436. doi:10.1007/s12599-016-0453-1.
- [3] H. Brignull, Deceptive patterns, 2023. [www.deceptive.design](http://www.deceptive.design).
- [4] M. Martini, C. Drews, P. Seeliger, Q. Weinzierl, *Zeitschrift für digitalisierung und recht* (2022).
- [5] J. Luguri, L. J. Strahilevitz, Shining a light on dark patterns, *Journal of Legal Analysis* 13 (2021) 43–109. doi:10.1093/jla/laaa006.
- [6] Q. Weinzierl, *Neue Zeitschrift für Verwaltungsrecht-Extra* (2020).
- [7] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, A. Narayanan, Dark patterns at scale: Findings from a crawl of 11k shopping websites, *Proceedings of the ACM on Human-Computer Interaction* 3 (2019) 1–32. doi:10.1145/3359183.
- [8] K. Bongard-Blanchy, A. Rossi, S. Rivas, S. Doublet, V. Koenig, G. Lenzini, "i am definitely manipulated, even when i am aware of it. it's ridiculous!"-dark patterns from the end-user perspective, in: *Designing Interactive Systems Conference 2021*, 2021, pp. 763–776. doi:10.1145/3461778.3462086.
- [9] F. J. Costello, J. Yun, K. C. Lee, Digital dark nudge: An exploration of when digital nudges unethically depart, in: *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2022. doi:10.125/79868.
- [10] R. H. Thaler, C. R. Sunstein, *Nudge*, PENGUIN BOOKS, 2021, pp. 6–8.
- [11] C. Meske, T. Potthoff, The dinu-model—a process model for the design of nudges, *Proceedings of the 25th European Conference on Information Systems (ECIS)* (2017).
- [12] P. Graßl, H. Schraffenberger, F. Zuiderveen Borgesius, M. Buijzen, Dark and bright patterns in cookie consent requests, *Journal of Digital Social Research* 3 (2021) 1–38. URL: <https://jdsr.se/ojs/index.php/jdsr/article/view/54>. doi:10.33621/jdsr.v3i1.54.
- [13] S. Schomberg, T. J. Barev, A. Janson, F. Hupfeld, Ansatz zur umsetzung von datenschutz nach der ds-gvo im arbeitsumfeld: Datenschutz durch nudging, *Datenschutz und Datensicherheit-DuD* 43 (2019) 774–780. doi:10.1007/s11623-019-1204-5.
- [14] watson.de, Green Nudging: Schon kleine Anreize bringen Menschen zum Energiesparen, 2022. [https://www.watson.de/!168653241?utm\\_medium=social-user&utm\\_source=social\\_app](https://www.watson.de/!168653241?utm_medium=social-user&utm_source=social_app), urldate = 2023-03-06.
- [15] A. Caraban, E. Karapanos, D. Gonçalves, P. Campos, 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction, in: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–15. doi:10.1145/3290605.3300733.
- [16] D. Djurica, K. Figl, The effect of digital nudging techniques on customers' product choice and attitudes towards e-commerce sites, *Americas Conference on Information Systems 2017* (2017) 1 – 7.
- [17] A. Kozyreva, S. Lewandowsky, R. Hertwig, Citizens versus the internet: Confronting digital challenges with cognitive tools, *Psychological Science in the Public Interest* 21 (2020) 103–156. doi:10.1177/1529100620946707.
- [18] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, et al., Nudges for privacy and security: Understanding and assisting users' choices online, *ACM Computing Surveys (CSUR)* 50 (2017) 1–41. doi:10.1145/3054926.
- [19] A. Mathur, M. Kshirsagar, J. Mayer, What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods, in: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–18. doi:10.1145/3411764.3445610.
- [20] N. C. on Informatics, L. (CNIL), Shaping choices in the digital world, 2020. [https://linc.cnil.fr/sites/default/files/atoms/files/cnil\\_ip\\_report\\_06\\_shaping\\_choices\\_in\\_the\\_digital\\_world.pdf](https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf), urldate = 2023-03-06.
- [21] M. Jesse, D. Jannach, Digital nudging with recommender systems: Survey and future directions,

- Computers in Human Behavior Reports 3 (2021). doi:10.1016/j.chbr.2020.100052.
- [22] C. Bösch, B. Erb, F. Kargl, H. Kopp, S. Pfattheicher, Tales from the dark side: Privacy dark strategies and privacy dark patterns., Proceedings on Privacy Enhancing Technologies 2016 (2016) 237–254. doi:10.1515/popets-2016-0038.
- [23] S. Greenberg, S. Boring, J. Vermeulen, J. Dostal, Dark patterns in proxemic interactions: a critical perspective, in: Proceedings of the 2014 Conference on Designing Interactive Systems, 2014, pp. 523–532. doi:10.1145/2598510.2598541.
- [24] N. C. Council, Deceived by design, how tech companies use dark patterns to discourage us from exercising our rights to privacy, Norwegian Consumer Council Report (2018). <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.
- [25] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, A. L. Toombs, The dark (patterns) side of ux design, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1–14. doi:10.1145/3173574.3174108.
- [26] C. M. Gray, S. S. Chivukula, A. Lee, What kind of work do " asshole designers " create? describing properties of ethical concern on reddit, in: Proceedings of the 2020 ACM Designing Interactive Systems Conference, 2020, pp. 61–73. doi:10.1145/3357236.3395486.
- [27] G. Conti, E. Sobiesk, Malicious interface design: Exploiting the user, in: Proceedings of the 19th International Conference on World Wide Web, 2010, pp. 271–280. doi:10.1145/1772690.1772719.
- [28] W. Lidwell, K. Holden, J. Butler, Universal principles of design, revised and updated: 125 ways to enhance usability, influence perception, increase appeal, make better design decisions, and teach through design, Rockport Pub, 2010.
- [29] A. Narayanan, A. Mathur, M. Chetty, M. Kshirsagar, Dark patterns: Past, present, and future: The evolution of tricky user interfaces, Queue 18 (2020) 67–92. doi:10.1145/3400899.3400901.
- [30] B. Morrison, C. Sengul, M. Springett, J. Taylor, K. Renaud, Mental models of dark patterns (2021). [https://spritehub.org/wp-content/uploads/2021/12/SPRITE\\_Lit\\_Review8.pdf](https://spritehub.org/wp-content/uploads/2021/12/SPRITE_Lit_Review8.pdf).