Website Operators are not the Enemy Either - Analyzing Options for Creating Cookie Consent Notices without Dark Patterns

Alina Stöver
alina.stoever@tu-darmstadt.de
Technische Universität Darmstadt

Nina Gerber
nina.gerber@tu-darmstadt.de
Technische Universität Darmstadt

Christin Cornel
Technische Universität Darmstadt

Mona Henz
Technische Universität Darmstadt

Karola Marky
karola.marky@itsec.uni-hannover.de
Leibniz Universität Hannover

Verena Zimmermann
verena.zimmermann@tu-darmstadt.de
Technische Universität Darmstadt

Joachim Vogt
joachim.vogt@tu-darmstadt.de
Technische Universität Darmstadt

ABSTRACT

Users frequently receive cookie consent notices when they enter a website. They are supposed to enable an informed decision about data collection. Instead, they often contain deceptive designs - also known as dark patterns - that can nudge users to consent and thus compromise their privacy. In this paper, we explore the causes of the widespread use of dark patterns in cookie consents. To do so, we take the perspective of website operators, who are responsible for the use of cookie consent notices and are increasingly making use of Consent Management Platforms (CMPs) to manage end-user consent. CMPs usually contain certain design templates. To find out whether it is possible for website operators to generate notices without dark patterns using CMPs, we analyzed a selection of the templates offered by major CMPs. We show that 60% of the notices created with default settings contain at least one dark pattern. A notice that does not nudge toward a certain choice could only be generated with 62.5% of the CMPs. Our results imply that the responsibility for privacy-friendly notices lies more with the CMPs than with the website operators.

KEYWORDS

Cookie consent notice, dark pattern, website operator, CMP (consent management platform), informed privacy decision, usable privacy

1 INTRODUCTION

"This website uses cookies that help the website to function and also to help us track how you interact with our website. But for us to provide the best experience, enable the specific cookies from Settings, and click on Accept." This exemplary notice shown in Figure 1 is probably close to what many users have read before when visiting a website. While the goal of cookie consent notices is enabling users to make an informed decision about data sharing, in reality cookie consent notices are often designed to encourage users to give consent as shown in Figure 1 by highlighting the "Accept all" button. Prior research demonstrated that such deceptive design choices, also known as dark patterns, can lead to increased user consent [76]. The resulting compromise of the users' privacy is potentially unintended in many cases. Previous research on cookie consent notices has primarily focused on the user's perspective and the challenges arising from integrated dark patterns [5, 34, 76]. However, it is the Website Operators (WOs) who are technically and legally responsible for designing and integrating cookie consent notices into their website if they use cookies. Therefore, the viewpoint of WOs and their impact on cookie consent notice design is at least equally important. At a first glance, it might be favorable for WOs to nudge users towards accepting all cookies by using a dark pattern as the collection of statistics and advertising data might be part of their business model. However, building trust and receiving positive user feedback on the website by being transparent about cookie use and allowing for an informed decision might be a relevant interest as well. From the WOs perspective, alternatives to dark patterns could be designs that do not deliberately encourage a certain choice (balanced designs) or cookie consent notices that even nudge users to refuse all cookies. The latter kind of notices are also labeled bright designs or bright patterns as a complement to the term dark pattern [34]. Yet, the notice design choices of WOs might not only be influenced by their interests but also by the services used to generate cookie consent notices. WOs increasingly make use of so-called Consent Management Platforms (CMPs) to create cookie consent notices. CMP "means the company or organisation that centralises and manages transparency for, and consent and objections of the end user" [25, p.6]. One reason for the use of CMPs is the promise to be on the safe side legally [35]. CMPs generally include certain design templates and restrictions. This leads to the question whether the use of CMPs and the related design templates influence the share of dark patterns in cookie consent notices. Our research questions (RQ) therefore are: **RQ1:** Do the default templates for cookie consent notices of the CMPs already contain dark patterns and if so, which ones? **RQ2:** Do the

MuC'22, 04.-07. September 2022, Darmstadt

https://doi.org/10.18420/muc2022-mci-ws01-458

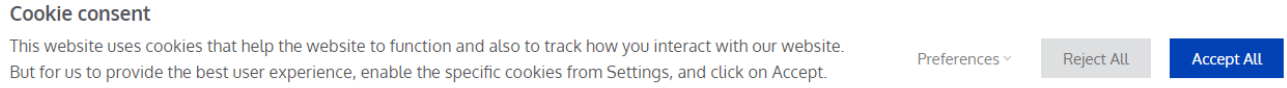


Figure 1: Cookie consent notice created using the template with default settings from www.cookie-yes.com [15]

templates for cookie consent notices of the CMPs allow to generate notices with balanced and/or bright design?

To target these questions, we analyzed the options for WOs to create cookie consent notices that do not include a dark pattern as well as options to even create a bright pattern. The contribution of our research is threefold: First, we provide insights from a WO perspective into cookie consent notice generation using CMPs. Thereby, our study is a first exploratory step to find possible explanations for the widespread use of dark patterns in cookie consent notices. Second, we show that notices often already contain dark patterns when created with the CMPs' default settings and that it is inconvenient to generate more privacy-friendly alternative notices. Third, from the findings we derive relevant implications for WOs and CMPs. Among others, we suggest that CMPs have a responsibility to enable WOs to generate privacy-friendly notices in general, i.e. notices that do not include dark patterns but transparently allow the users to make an informed decision. This opens up a number of exciting research opportunities, such as long-term studies or deeper analyses of the interests and needs of WOs in general as well as in comparison to the users' perspective.

2 RELATED WORK

This section gives an overview of the related work. We start with the general definition of dark patterns and related taxonomies. This is followed by related work on dark patterns in cookie consent notices and particularly in CMPs.

Dark Pattern - According to Brignull´s website [7] "deceptive design practices (also known as "dark patterns") are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something." Mathur et al. [48, p.81] define dark patterns as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions.". In the case of cookie consent notices, this means buttons, structure, and labels are purposefully designed to lead website visitors to make privacy-unfriendly choices and potentially act against their own interests [23]. Previous research has already identified a large number of dark pattern types [49]. A taxonomy of dark pattern strategies that have already been investigated in the context of cookie consent notices [65] is provided by Gray et al. [32]. They derive a total of five dark pattern strategies from the literature, which are listed in Table 1. Starting with these strategies, we have derived definitions for the cookie consent notice context that provide the basis for our notice analysis (see Section 3).

Dark Patterns in Cookie Consent Notices - Several studies have explored the prevalence of dark patterns in EU-based website cookie consent notices and indicated that obstruction and interface interference are the most frequent dark patterns [38, 41, 65]. Prior research shows that cookie consent notice design greatly affects the extent to which website visitors consent to the use of cookies [5, 34, 44, 45, 52, 76]. Dark patterns, i.e., designs that aim to nudge users towards consenting to all cookies have repeatedly been found to increase cookie acceptance rates. These designs include, among others, making the rejection of cookie use more difficult than the acceptance (obstruction), e.g., by hiding the reject button on a deeper layer [45, 52], or displaying the acceptance button more prominently than the rejection button (interface interference), e.g., by color-highlighting it [44, 76].

Still, there are mixed results regarding the level to which particular dark patterns affect the users' cookie consent response. For example, Grassl et al. [34], who also studied the effect of dark patterns, found no significant influence of obstruction (in this case, hiding the reject button on a second layer) and interface interference (in this case, color-highlighting the accept button) on acceptance rates. This may be due to the fact that even in their baseline condition most participants agreed to the use of cookies. However, when the dark patterns were reversed to nudging users towards rejecting cookie use (so-called "bright pattern"), they found significant effects for obstruction, but not for interface interference. In Fernandez et al.'s [5] study, interface interference (color-highlighting the accept button) did not lead to more participants changing the default settings either.

Gray et al. [33] discuss the implications of dark patterns in cookie consent notices they observed in the wild from a HCI, design, privacy protection, and legal perspective. In terms of interface design, they focus on design elements that apply a hierarchy of choice options or make one option more salient and attractive than another. The authors conclude that due to the variety of implementation options, it is impossible to fully examine and evaluate the different possible design elements from both a legal and a user perspective.

Dark Patterns in Cookie Consent Notices of CMPs - For the creation of cookie consent notices for their website, WOs are increasingly using CMPs, probably because they promise them legal compliance. Based on 161 million browser crawls, Hils et al. [35] estimate that CMP adoption doubled between June 2018 and 2019 and then doubled again by June 2020 whereby CMPs were mainly used on medium popular websites [35]. Other studies focused on how cookie consent notices implemented by using popular CMPs comply with legal requirements and, in case of non-compliance, which dark pattern they included [20, 52]. In 2019, Nouwens et al. [52] evaluated the designs of the most frequently used CMPs (Cookiebot [11], Crownpeak [16], OneTrust [54], QuantCast [59], TrustArc [72]) in the UK against the General Data Protection Regulation (GDPR) and ePrivacy Directive by scraping the implementations of cookie consent notices created with these CMPs on the 10,000 most visited websites in the UK. They found that less than 12% of the considered cookie consent notices met the minimum requirements defined by Nouwens et al. [52] to comply with European legal requirements:

Table 1: The table provides an overview of the five dark pattern strategies derived from Gray with Gray's corresponding definitions as well as definitions we have adapted for the cookie consent context.

Dark pattern strategies	Definition according to Gray [32]	Definition adopted for consent context
Interface Interference	Manipulation of the user interface that privileges certain actions over others [32, p.5]	The design (color, font, size) of the buttons for accepting and rejecting cookies are not equivalent.
Obstruction	Making a process more difficult than it needs to be, with the intent of dissuading certain action(s) [32, p.5]	The option to reject all cookies is not available on the first page of the notice.
Forced Action	Requiring the user to perform a certain action to access (or continue to access) certain functionality [32, p.5]	Users can enter the website only after interacting with the notice.
Sneaking	Attempting to hide, disguise, or delay the divulging of information that is relevant to the user [32, p.5]	Users unknowingly agree to cookies (e.g. because notice requires opt-out).
Nagging	Redirection of expected functionality that persists beyond one or more interactions [32, p.5]	After their decision, users are asked again by a notice whether they want to stay with the decision.

(1) consent must be given explicitly (e.g., by clicking on a button rather than continue to browse the website), (2) accepting all must be as easy as rejecting all (e.g., the reject all button has to be on the same layer as the accept all button – this corresponds to Gray et al.'s obstruction dark pattern [32]), (3) the notice must not contain pre-ticked boxes (i.e., opt-in instead of opt-out). Their results suggest that cookie consent notices do often not comply with the last two requirements, since the reject all button is harder to access than the accept all button, and detailed cookie settings often rely on an opt-out procedure. Nouwens at al. [52] also examined two CMPs that we considered in our study: QuantCast, which was associated with the highest number of minimally compliant cookie consent notices (26%) due to always asking for explicit consent and a low number of pre-ticked boxes; and Cookiebot, which had the second most minimal compliant cookie consent notices (6%). Degeling et al. [20] analyzed 6,579 of the most popular websites in different EU countries in 2017 and 2018 after the GDPR came into force. They found that most of the frequently used CMPs (as indicated by their crawling-based analysis of EU websites) do not support the technical properties necessary to comply with GDPR requirements for cookie consent notices. However, in this study, they did not evaluate the prevalence of dark patterns, but focused on technical aspects such as whether cookie consent libraries (including CMPs) allow to reject cookie use or to ask for consent for different cookie categories (i.e., cookies used for different purposes that are often associated with the collection of different types of data). Matte et al. [50] crawled 1,426 websites containing cookie consent notices which are implemented by CMPs that take part in the Interactive Advertising Bureau (IAB) Transparency and Consent Framework. While they found at least one legal violation in more than half of the websites, they did not analyze the cookie consent notices with respect to the dark patterns considered in our study. In a recent study, Bollinger et al. [6] extended this analysis by crawling 30,000 websites, and found violations in more than 90% in the analyzed cookie consent notices.

3 METHOD

To achieve our research goal, we proceeded in three steps: (1) identification of relevant CMPs, (2) creation of cookie consent notices with identified CMPs, and (3) qualitative analysis of the generated cookie consent notices.

Step 1: Identification of relevant CMPs - Selecting the most relevant CMPs is a tricky task, because different top lists exist [28, 31, 40]. Hils et al.'s [35] analyses show that the market share of different CMPs is very dynamic and varies depending on the websites analyzed. For our study, we decided to merge sources (top lists, related work, and our own google search) of CMPs to generate a comprehensive list of CMPs (see Appendix A).

Step 2: Creation of cookie consent notices - The goal of Step 2 was to generate different cookie consent notices using the CMPs identified in Step 1. For this purpose, two independent researchers were instructed to put themselves in the perspective of WOs and to generate three cookie consent notices using the templates of the CMPs (see Appendix A). We decided to have the cookie consent notices created by two independent researchers to increase the quality of the data. The cookie consent notices generated in this way were compared by a third person. Since our predefined procedure was only standardized to a certain degree and the CMP websites were often confusing, not all results were identical (e.g. there were differences in the background color). The differences were discussed in the group of researchers and in case of marginal differences (e.g. different fonts) a design variant was selected as the basis for the analysis. In one case (CCM [8]), however, the results were so different that all variants were included in the further analysis process. For a better overview, however, only the variant with the most dark patterns was included in the final evaluation. The creation of the cookie consent notices took place during the period of March 10-11, 2022. For the purpose of comparability, we selected all CMPs that were free of charge and that did not require a personal contact with the sales department from the resulting list of CMPs. In total, 15 of the 49 CMPs met this requirement (see Appendix B). The following three types of notices were generated when possible:

(1) *Default notice:* The notice was set to be GDPR-compliant and in English, otherwise the default settings were used.
(2) *Balanced notice:* Here, the goal was to generate a notice where the buttons that accept and reject cookies are placed equally (size, color, position) on the first page of the notice.
(3) *Bright notice:* In the sense of Grassl et al. [34] this notice should nudge users to reject all cookies. For this purpose, the "reject all" button should be visually prominent.

Step 3: Analysis of Cookie Consent Notices - In Step 3, the cookie consent notices generated in Step 2 were analyzed by two independent raters, who were not involved in the notice creation. For this purpose, they received screenshots of the balanced and default cookie consent notice, without the information which notice referred to which case. The raters were provided with Gray et al.s´ [32] dark pattern taxonomy and our adapted definitions

(see Table 1). In the analysis, the focus was on the dark patterns obstruction and interface interference, which Soe et al. [65] had identified as the most common dark patterns in cookie consent notices. The raters were asked to rate the notices in terms of the following aspects:

(1) *Obstruction:* Does the notice contain obstruction? [*yes, no, inconclusive*]
(2) *Interface Interference:* Does the notice contain interface interference? [*yes, no, inconclusive*]
(3) *Other Dark Patterns:* Does the notice contain other dark patterns? [*yes, no, inconclusive*]
(4) *Overall Rating:* Are there any dark patterns in the notice? [*yes, no, inconclusive*]
(5) *Number Dark Pattern*: How many dark patterns does the notice contain?

In addition, the raters could comment on the cookie consent notices. After the raters had completed their ratings, they were compared by a third researcher. Discrepancies in the ratings were solved by discussion with the raters.

4 RESULTS

Starting point of this research were the questions, whether the default notices of CMPs already contained dark patterns, and if so, which ones and whether the creation of balanced and bright notices was possible at all. In total, we looked at 15 CMP providers. From each of these CMP providers, one default (15 in total) and, if possible, one balanced (12 in total) as well as one bright (10 in total) cookie consent notices were included in the results. In the following, we report the results of our notice analyses and supplement them with further observations that we made while creating and analyzing the notices.

4.1 Default Cookie Consent Notice

In this section, we address the analyses related to our research question 1: Do the default templates for cookie consent notices of the CMPs already contain dark patterns and if so, which ones?

4.1.1 Dark Pattern: Obstruction and Interface Interference. First, we looked at the default templates for cookie consent notices in terms of the two dark patterns that occur most often in cookie consent notices according to Soe et al. [65]: Interface interference and obstruction. For an overview of the results, see Figure 2a. The analysis shows that 9 of 15 of the templates contain at least one of these two dark patterns. Interface interference occurs most frequently (8 out of 15). Figure 3a provides an example for a notice with interface interference. Obstruction was only clearly identified in one of the templates (see Figure 3b), which is a possible GDPR violation [52].

4.1.2 Other Patterns. We also looked at the default templates for cookie consent notices to see if they contained any dark patterns other than obstruction and interface interference. In 12 of the 15 notices analyzed, the raters saw the possibility of sneaking and/or forced action. For example, the button "Accept" (see Figure 3b) might contain forced action, depending on what is hidden behind the button "My Options". Some notices might contain "sneaking" if users are not aware of the consequence of their choice "Accept all" (e.g. in Figure 4). In addition, the raters noticed that only 2 of the 15 notices allowed personalized settings on the first layer of the cookie consent notice.

4.2 Balanced and Bright Cookie Consent Notices

In this section, we address the analyses related to our research question 2: Do the templates for cookie consent notices of the CMPs allow to generate notices with a balanced and/or bright design? Furthermore, we were interested in whether it is possible to generate balanced and bright cookie consent notices using the templates of the CMPs. For an overview of the results, see Figure 2b. In balanced notices, it is possible to select the same design for the agree and disagree buttons. This was possible with 10 out of 15 of the CMPs. An example of a balanced notice can be found in Figure 4. A template for cookie consent notice was considered as bright, when the button to reject cookies could be visually highlighted. This was possible with 10 out of 15 of the CMPs. An example of a balanced notice can be found in Figure 5.

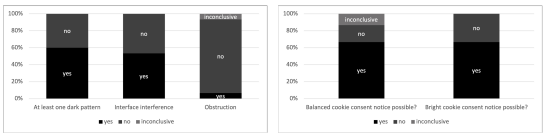
4.3 Observations during Cookie Consent Notice Creation

During the creation of the notices, we recognized a few things that we would like to report here: *Challenges for balanced and bright notice creation:* The creation of balanced and/or bright notices was partly only possible with a premium account (e.g., using the CMP Cookie Hub [13]). In another case, the creation was generally possible, but very inconvenient. For example, in the template of the CMP SmartLife [64], the possibility to customize the color of the buttons was hidden behind a layer. *Dark patterns on CMPs websites:* We also noticed that some of the CMPs' websites (e.g., SmartLife [64]) were designed in such a way that they firmly nudged WOs to buy products. In addition, we were often not aware of the actual consequences of different settings we made on notices. For example, when generating a notice using the CMP CCM19 [8], it was not clear for which button we were changing the color.

5 DISCUSSION

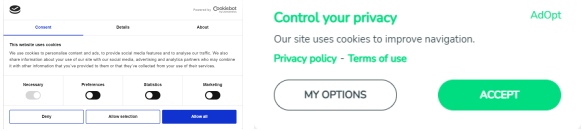
The aim of our study was to find answers to the following two research questions: (RQ1:) Do the default templates for cookie consent notices of the CMPs already contain dark patterns and if so, which ones? (RQ2:) Do the templates of the CMPs allow to generate notices with balanced and/or bright design? To investigate this, we analyzed the templates of 15 CMPs. Previous studies have examined how cookie consent notices were actually implemented on websites using a CMP [38, 52, 65]. In the following, we will relate our results to these studies. We derive the following three learnings from our study. Learning 1 and 2 relate to our research questions.

Learning 1: Default notices often contain dark patterns (RQ1). Our analysis of the notices with respect to the dark patterns listed in Gray et al.'s [32] taxonomy shows that the interface interference pattern is the most common in the CMP templates with 53.33%. This is consistent with the results of the analyses of cookie consent notices in the field [65]. This match could be an indicator that many WOs directly use the templates with default settings that contain dark patterns. Overall, we were able to show that 60% of the default templates for cookie consent notices definitely contain



(a) (b)

Figure 2: (a) Results of the analysis of the cookie consent notices using the CMP templates (*N=15)* with default settings, (b) Results of the analysis of the CMP templates (*N=15)* regarding whether balanced and bright cookie consent banners can be generated.



(a) (b)

Figure 3: (a) Cookie consent notice generated using templates with default settings (a) from Cookiebot [11] containing interface interference, (b) from adopt [3] containing obstruction.

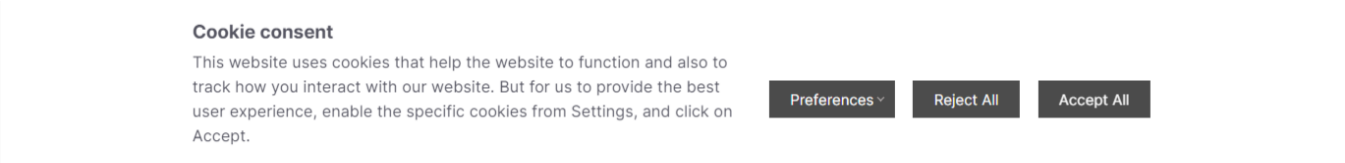


Figure 4: A balanced cookie consent notices design generated using the template of the CMP Cookie Yes [15]

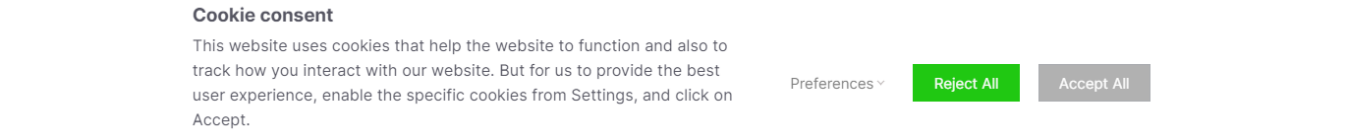


Figure 5: A bright cookie consent notices design generated using the template of the CMP Cookie Yes [15]

a dark pattern. That is less compared to analyses in the field [38, 52, 65]. There are three possible explanations for this. (1) In our study, we only analyzed the notices of CMPs that were free of charge. Thus, we do not cover all CMPs analyzed in related work. (2) Hils et al. [35] was able to show in his study that the CMP industry is very dynamic. This may be the reason why old versions of the notices are still available on the web or the analyses of related work might be already outdated. (3) Another possibility why we found fewer dark patterns than other studies could be that not all WOs use the default cookie consent notices of the CMPs, but possibly integrate dark patterns themselves. So far, there is no research that comprehensively examines the interests of WOs in cookie consent.

Learning 2: Creating privacy-friendly notices is often impossible or inconvenient (RQ2). We were able to generate balanced and bright notices for only 62.5% of the CMPs. For the CMPs that allowed this, it was sometimes very inconvenient. This is problematic because previous research has shown that WOs often have to handle many different tasks, whereby especially for smaller or medium-sized websites, operating the website is not their primary task. Furthermore, WOs often lack awareness of privacy issues and knowledge about implementation [43]. Therefore, they rely on transparent working practices from third party vendors, such as CMPs. However, it is not always clear which interests the CMPs are pursuing.

Learning 3: CMPs may have a large influence on which dark pattern in cookie consent notices are widespread on the web. Hils et al. [35] showed that notices from CMPs are becoming increasingly widespread, so their influence is obviously increasing. Especially when dominant CMPs promote dark patterns, this can be critical for the privacy of end users. For example, the German market leader "Cookiebot by Usercentrics" [11] does not allow the interface interference to be switched off in the free version. This means that even if WOs wanted to create privacy-friendly notices, it would often be impossible or challenging for them with a CMP. This could be a

possible explanation why dark patterns in cookie consent notices are still so widespread.

In summary: Dark patterns in the default templates of CMPs are widespread, even if WOs are motivated to generate notices without dark patterns this is partly not possible. Therefore it is important to empower WOs to choose CMPs whose templates do not contain dark patterns. We also conclude that an urgent step to eventually protect the privacy of end users is to hold CMPs accountable, because WOs are also reliant on them.

6 LIMITATIONS AND FUTURE WORK

Our study has an exploratory character, which brings some limitations. At the same time, our results serve as a starting point for exiting avenues for future research. Both, limitations and how they can be addressed in future work, are described in the following: *Identification of relevant CMPs with web crawlers:* The market share of CMPs is very dynamic and also depends on the website size [35]. We derived the relevance of the CMPs analyzed based on existing literature, which may not reflect the current state. Therefore, in the future, the relevant CMPs should be identified again with the help of a web crawler. *Extensive analyses of the offers of all relevant CMPs:* In this study, we only examined notices from CMPs that were free of charge and did not require a personal contact with the sales department from the resulting list of CMPs. Thus, our results are not representative of all relevant CMPs. In order to create a better generalizability, all relevant CMPs should be analyzed if possible. It may be necessary to use a cover story for this purpose in order not to bias the CMPs when contacting them. *Analyses of implemented cookie consent notices:* We have only analyzed screenshots of the templates for cookie consent notices and not the actual notices implemented in a website. Thus, the raters could not interact with the cookie consent notices and it was sometimes difficult for them to assess to what extent dark patterns, such as sneaking or forced action, were included in the notices. Future research should actually implement the notices in websites to perform deeper analysis. *Long-term study of default cookie consent notices:* It should also be noted that the templates we analyzed in our study, only represent a snapshot of March 2022. Hils et al. [35] had already shown that the CMP industry is very dynamic, and the relevance of individual CMPs and the design of the notices could change in the future. It would be interesting to analyze whether and how (e.g., influenced by external events such as changes in the law or court rulings) the CMPs adapt their templates. *Involvement of WOs:* In our study, we tried to take the perspective of WOs. However, future research should explore their perspective, interests and needs in more detail. This could be done by directly interviewing people who operate websites or by involving them in the generation of notices with the help of CMPs. *Deeper Analysis of CMP websites:* When generating the notices, we already noticed that this was often inconvenient or that the websites of the CMPs contained dark patterns. In order to gain a deeper understanding of CMPs, it might be worthwhile to take a closer look at the user experience of their websites. For example, duration, clicks and workload could be measured when generating default and neutral cookie consent notices as such or in comparison to the creation of dark patterns. *Further questions:* Finally, our study raised a number of other fundamental questions. Regarding the design of cookie consent notices, the question arises how solutions look like that connect the interests of WOs and users? Regarding the CMPs, the question arises how they can be held more accountable in the future.

ACKNOWLEDGMENTS

This work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, grant number 251805230/GRK 2050) and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

REFERENCES

[1] 2BAdvice. 2022. 2BAdvice. Retrieved on March 23, 2022 from https://www.2b-advice.com/de/.
[2] Commanders Act. 2022. Commanders Act. Retrieved on March 23, 2022 from https://www.commandersact.com/de/.
[3] AdOpt. 2022. AdOpt. Retrieved on March 23, 2022 from https://goadopt.io/.
[4] axeptio. 2022. axeptio. Retrieved on March 23, 2022 from https://www.axeptio.eu/en/home.
[5] Carlos Bermejo Fernandez, Dimitris Chatzopoulos, Dimitrios Papadopoulos, and Pan Hui. 2021. This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 346 (oct 2021), 22 pages. https://doi.org/10.1145/3476087
[6] Dino Bollinger, Karel Kubicek, Carlos Cotrini, and David Basin. 2022. Automating Cookie Consent and GDPR Violation Detection. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, USA, 1–18. https://www.usenix.org/conference/usenixsecurity22/presentation/bollinger
[7] Harry Brignull. 2022. Deceptive Design. Retrieved on March 28, 2022 from https://www.deceptive.design.
[8] CCM19. 2022. CCM19. Retrieved on March 23, 2022 from https://www.ccm19.de/cookie-banner.html.
[9] Google Funding Choices. 2022. Google Funding Choices. Retrieved on March 23, 2022 from https://fundingchoices.google.com/start/?authuser=0.
[10] consent manager. 2022. consent manager. Retrieved on March 23, 2022 from https://www.consentmanager.de/.
[11] Cookiebot. 2022. Cookiebot by Usercentrics. Retrieved on March 23, 2022 from https://www.cookiebot.com/de/.
[12] COOKIEFIRST. 2022. COOKIEFIRST. Retrieved on March 23, 2022 from https://cookiefirst.com/de/consent-management-platform/.
[13] CookieHub. 2022. CookieHub. Retrieved on March 23, 2022 from https://www.cookiehub.com/de.
[14] CookiePro. 2022. CookiePro by OneTrust. Retrieved on March 23, 2022 from https://www.cookiepro.com/.
[15] CookieYes. 2022. CookieYes. Retrieved on March 23, 2022 from https://www.cookieyes.com/consent-management-platform/.
[16] crownpeak. 2022. crownpeak. Retrieved on March 23, 2022 from https://www.crownpeak.com//.
[17] DataGrail. 2022. DataGrail. Retrieved on March 23, 2022 from https://www.datagrail.io//.
[18] Datenschutz-Generator.de. 2022. Datenschutz-Generator.de. Retrieved on March 23, 2022 from https://datenschutz-generator.de/.
[19] DATEV. 2022. DATEV. Retrieved on March 23, 2022 from https://www.datev.com/about-datev/data-protection/.
[20] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Network and Distributed System Security Symposium (NDSS 2019)*. Internet Society, Reston, VA, USA. https://doi.org/10.14722/ndss.2019.23378
[21] devowl.io. 2022. devowl.io. Retrieved on March 23, 2022 from https://devowl.io/de/wordpress-real-cookie-banner/.
[22] Didomi. 2022. Didomi. Retrieved on March 23, 2022 from https://www.didomi.io/de/.
[23] dpa. 2021. Datenschützer starten Beschwerdewelle gegen Cookie-Banner. Retrieved on March 28, 2022 from https://www.sueddeutsche.de/service/internet-datenschuetzer-starten-beschwerdewelle-gegen-cookie-banner-dpa.urn-newsml-dpa-com-20090101-210531-99-801337.
[24] ethyca. 2022. ethyca. Retrieved on March 23, 2022 from https://ethyca.com/.
[25] IAB Europe. 2019. *Transparency & Consent Framework – Policies Version 2020-08-24.3.2.* IAB Europe. www.iabeurope.eu Retrieved on March 28, 2022

from https://iabeurope.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf.
[26] Evidon. 2022. Evidon by Crownpeak. Retrieved on March 23, 2022 from https://www.evidon.com/.
[27] PrivacyUX for CCPA. 2022. PrivacyUX for CCPA. Retrieved on March 23, 2022 from https://www.privacyux.com/.
[28] G2. 2022. Best Consent Management Platforms. Top 30 scored CMPs retrieved on March 28, 2022 from https://www.g2.com/categories/consent-management-platform-cmp.
[29] google. 2022. Google Search 1. Results provided on page 1-4 of our Google search in incognito mode for the term "Consent Management Platform" on March 10th 2022..
[30] google. 2022. Google Search 2. Results provided on page 1-4 of our Google search in incognito mode for the term "cookie consent notice" on March 10th 2022..
[31] Lisa Gradow and Ramona Greiner. 2021. *Quick Guide Consent-Management*. Springer Gabler, Wiesbaden, Germany.
[32] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. *The Dark (Patterns) Side of UX Design*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108
[33] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 2021. *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective*. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3411764.3445779
[34] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. 2021. Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research* 3, 1 (Feb. 2021), 1–38. https://doi.org/10.33621/jdsr.v3i1.54
[35] Maximilian Hils, Daniel W Woods, and Rainer Böhme. 2020. Measuring the emergence of consent management on the web. In *Proceedings of the ACM Internet Measurement Conference*. ACM, New York, NY, USA, 317–332.
[36] Salesforce Identity. 2022. Salesforce Identity. Retrieved on March 23, 2022 from https://www.salesforce.com/de/?ir=1.
[37] iubenda. 2022. iubenda. Retrieved on March 23, 2022 from https://www.iubenda.com/en/.
[38] Georgios Kampanos and Siamak F. Shahandashti. 2021. Accept All: The Landscape of Cookie Banners in Greece and the UK. In *ICT Systems Security and Privacy Protection*, Audun Jøsang, Lynn Futcher, and Janne Hagen (Eds.). Springer International Publishing, Cham, 213–227.
[39] Ketch. 2022. Ketch. Retrieved on March 23, 2022 from https://www.ketch.com/.
[40] Kevel. 2022. Consent Management Platform (CMP) 2022 Tracker. Retrieved on March 28, 2022 from https://www.kevel.com/cmp/.
[41] Chiara Krisam, Heike Dietmann, Melanie Volkamer, and Oksana Kulyk. 2021. *Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3481357.3481516
[42] LiveRamp. 2022. LiveRamp. Retrieved on March 23, 2022 from https://liveramp.com/blog/consent-management-platform-cmp/.
[43] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. 2021. Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support. In *30th USENIX Security Symposium (USENIX Security 21)*. Usenix, Berkeley, CA, USA, 2489–2506.
[44] Dominique Machuletz and Rainer Böhme. 2020. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 481–498. https://doi.org/10.2478/popets-2020-0037
[45] Stefan Mager and Johann Kranz. 2021. On the Effectiveness of Overt and Covert Interventions in Influencing Cookie Consent: Field Experimental Evidence. In *ICIS 2021 Proceedings (ICIS)*. AIS, Atlanta, GA, USA. https://aisel.aisnet.org/icis2021/cyber_security/cyber_security/5
[46] Mainwebsolutions. 2022. Mainwebsolutions. Retrieved on March 23, 2022 from https://www.cookie-banner-dsgvo.de/.
[47] Data Privacy Manager. 2022. Data Privacy Manager. Retrieved on March 23, 2022 from https://dataprivacymanager.net/consent_management_platform/.
[48] Arunesh Mathur, Gunes Acar, Michael J Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–32.
[49] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. 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*. ACM, New York, NY, USA, 1–18.
[50] Célestin Matte, Nataliia Bielova, and Cristiana Santos. 2020. Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, USA, 791–809. https://doi.org/10.1109/SP40000.2020.00076
[51] monsido. 2022. monsido. Retrieved on March 23, 2022 from https://monsido.com/solutions.
[52] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321
[53] ogury. 2022. ogury. Retrieved on March 23, 2022 from https://ogury.com/.
[54] OneTrust. 2022. OneTrust. Retrieved on March 23, 2022 from https://www.onetrust.com/solutions/consent-management-platform/.
[55] osano. 2022. osano. Retrieved on March 23, 2022 from https://www.osano.com//.
[56] Secure Privacy. 2022. Secure Privacy. Retrieved on March 23, 2022 from https://secureprivacy.ai/.
[57] PrivacyPolicies. 2022. PrivacyPolicies. Retrieved on March 23, 2022 from https://www.privacypolicies.com/de/.
[58] Piwik PRO. 2022. Piwik PRO. Retrieved on March 23, 2022 from https://piwik.pro/blog/consent-management-platforms-comparison/.
[59] Quantcast. 2022. Quantcast. Retrieved on March 23, 2022 from https://www.quantcast.com/products/choice-consent-management-platform/.
[60] Cookie Script. 2022. Cookie Script. Retrieved on March 23, 2022 from https://cookie-script.com/consent-management-platform.
[61] securiti. 2022. securiti. Retrieved on March 23, 2022 from https://securiti.ai/.
[62] Segment. 2022. Segment. Retrieved on March 23, 2022 from https://segment.com/.
[63] WS02 Identity Server. 2022. WS02 Identity Server. Retrieved on March 23, 2022 from https://wso2.com/identity-server/.
[64] SmartLife. 2022. SmartLife. Retrieved on March 23, 2022 from https://www.smartlife-online.de/cb/.
[65] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. *Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3419249.3420132
[66] Sourcepoint. 2022. Sourcepoint. Retrieved on March 23, 2022 from https://www.sourcepoint.com/de/dialogue-consent-management-platform-cmp/.
[67] Squarespace. 2022. Squarespace. Retrieved on March 23, 2022 from https://support.squarespace.com/hc/de.
[68] Termly. 2022. Termly. Retrieved on March 23, 2022 from https://termly.io/.
[69] Privacy tools. 2022. Privacy tools. Retrieved on March 23, 2022 from https://privacytools.com.br/.
[70] Transcend. 2022. Transcend. Retrieved on March 23, 2022 from https://transcend.io/.
[71] TRUENDO. 2022. TRUENDO. Retrieved on March 23, 2022 from https://www.truendo.com/.
[72] TrustArc. 2022. TrustArc. Retrieved on March 23, 2022 from https://trustarc.com/.
[73] TrustCommander. 2022. TrustCommander. Retrieved on March 23, 2022 from https://www.commandersact.com/de/loesungen/trustcommander/.
[74] UniConsent. 2022. UniConsent. Retrieved on March 23, 2022 from https://www.uniconsent.com/.
[75] usercentrics. 2022. usercentrics. Retrieved on March 23, 2022 from https://usercentrics.com/de/.
[76] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212

A CMP LIST

Table 2: The table shows a list of CMPs and their appearance various sources. Status refers to whether it was possible to generate a banner free of charge and without personally contacting a sales person. CMPs whose templates were included in the final analyses are marked in bold.

CMP	google search [29]	google search [30]	Kevel toplist [40]	G2 toplist [28]	Nouwens et al. [52]	Gradow et al. [31]	Status
2badvice [1]	✓						
AdOpt [3]				✓			✓
Axeptio [4]				✓			✓
CCM 19 [8]		✓					✓
Commanders Act [2]						✓	
consent manager [10]	✓	✓				✓	✓
Main web solution [46]		✓					
smart life [64]		✓					✓
Cookie Script [60]	✓						✓
Cookie yes [15]		✓		✓			✓
Cookiebot [11]	✓	✓	✓	✓	✓	✓	✓
cookiefirst [12]	✓						
CookieHub [13]	✓			✓			✓
CookiePro [14]				✓			✓
Crownpeak [16]			✓	✓	✓	✓	
data privacy manager [47]	✓						
DataGrail [17]				✓			
Datenschutzgenerator [18]		✓					
Datev [19]				✓			
Didomi [22]	✓			✓		✓	
Ethyca [24]				✓			
Evidon/Crownpeak [26]						✓	
google funding Choices [9]			✓				
Iubenda [37]	✓	✓	✓	✓		✓	✓
Ketch [39]				✓			
Liveramp [42]	✓		✓			✓	
Monsido[51]				✓			
Ogury [53]						✓	
onetrust [54]			✓	✓	✓	✓	
Osano [55]	✓		✓	✓		✓	
PiWik Pro [58]		✓		✓		✓	✓
privacy policies [57]		✓					
privacy tools [69]				✓			
PrivacyUX for CCPA [27]				✓			
Quantcast [59]	✓		✓	✓	✓	✓	✓
real cookie banner/**devowl** [21]		✓					✓
salesforce identity [36]				✓			
secure Privacy [56]				✓			
securiti [61]	✓			✓			
segment [62]				✓			
sourcepoint [66]	✓		✓			✓	
squarespace [67]		✓					
Termly.io [68]				✓			✓
Transcend [70]				✓			
truendo [71]	✓						
TrustArc [72]			✓	✓	✓	✓	
trustcommander [73]	✓						
uniconsent [74]	✓						
Usercentrics [75]	✓	✓		✓		✓	
WS02 Identiy Server [63]				✓			

B RESULTS OF CMP TEMPLATES ANALYSIS

Table 3: The table shows the results of the analyzed templates of 15 CMPs. With (1) balanced cookie consent notices possible (2) bright cookie consent notice possible (3) template with default settings contains dark pattern obstruction (4) template with default settings contains dark pattern interface interference (5) template with default settings contains at least one dark pattern (obstruction or interface interference)

CMP	(1) balanced	(2) bright	(3) obstruction	(4) interface interference	(5) at least one dark pattern
AdOpt [3]	no	no	yes	no	yes
Axeptio [4]	yes	yes	no	yes	yes
CCM 19 [8]	yes	yes	no	yes	yes
consent manager [10]	yes	yes	no	no	no
smart life [64]	inconclusive	yes	inconclusive	yes	yes
Cookie Script [60]	no	yes	no	yes	yes
Cookie Yes [15]	yes	yes	no	yes	yes
Cookiebot [11]	no	no	no	yes	yes
CookieHub [13]	yes	no	no	no	no
CookiePro [14]	yes	no	no	no	no
Iubenda [37]	yes	yes	no	no	no
PiWik Pro [58]	yes	yes	no	no	no
Quantcast [59]	yes	yes	no	yes	yes
devowl [21]	inconclusive	yes	no	yes	yes
Termly.io [68]	yes	no	no	no	no