Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites

CHIARA KRISAM, Karlsruhe Institute of Technology (KIT), Germany
HEIKE DIETMANN, Karlsruhe Institute of Technology (KIT), Germany
MELANIE VOLKAMER, Karlsruhe Institute of Technology (KIT), Germany
OKSANA KULYK, IT University of Copenhagen, Denmark

Cookie disclaimers are these days an indispensable part of surfing and working on the Internet. In this work, we report on examining and classifying the cookie disclaimers on the 500 most popular websites in Germany, based on the presented information about data collection via cookies and the provided choices at the cookie disclaimer. Our analysis results in 13 categories of cookie disclaimers, consisting of six main categories and additional subcategories. Our findings include that dark pattern based categories were prevalent among the cookie disclaimers: e.g. (1) more than 85% of the investigated websites providing a cookie disclaimer and giving the option to reject cookies are visually nudging users towards accepting all cookies; (2) Only 21.5% of those providing a cookie disclaimer offer a reject-all option with a single click. We discuss our results and conclude that both raising user awareness as well as addressing dark patterns from a legal point of view is needed.

ACM Reference Format:
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. In *European Symposium on Usable Security 2021 (EuroUSEC '21), October 11–12, 2021, Karlsruhe, Germany*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3481357.3481516

1 INTRODUCTION

Privacy implications of web tracking has been a topic of both academic research and public discussion for a long time, especially since May 25, 2018, the day from which the European General Data Protection Regulation (GDPR) [21] came into force. In particular, the cookie disclaimers present on websites are meant to inform the user about data collection and, if needed, to obtain their consent to it. However, these disclaimers manifest a conflict between convenience and privacy, with users having to make a decision when they visit a new website: Should they click whatever button they see first that would get rid of the disclaimer and allow them to browse the website, or should they search for an option to limit the sharing of their data, often having to click through the countless settings in order to do so. Such decisions are furthermore often exacerbated by the use of so-called dark patterns by the website providers that nudge the user into sharing more data via deceptive user interface elements. While the effects of dark patterns on user decisions has been a topic of investigation of several academic papers [9, 16, 18], and a subject for legal concern in several countries resulting in guidelines limiting their use [2, 5, 6], the extent to which dark patterns are still prevalent on common websites is yet unclear.

This paper aims to investigate the usage of dark patterns on most popular websites in Germany (Top 500 according to the Alexa rating). In particular, our contribution is three-fold: (1) based on the results from examining the websites, proposing a categorisation of cookie disclaimer designs (consisting of a total of 13 categories), that can be used as a baseline for further research on dark patterns and usable privacy; (2) providing an overview of designs most commonly used on top websites in Germany, as well as evaluating their privacy-friendliness and legal compliance; (3) discussing our findings in particular wrt. nudging users towards accepting all cookies (or more than needed).

EuroUSEC '21, October 11–12, 2021, Karlsruhe, Germany

ACM ISBN 978-1-4503-8423-0/21/10…$15.00
https://doi.org/10.1145/3481357.3481516

2 LEGAL BACKGROUND

Even if a cookie alone is not sufficient to identify a user, according to Recital 30 of the General Data Protection Regulation (GDPR)[21], cookies can be used "to create profiles of the natural persons and identify them". Thus, according to Article 4 No. 1 of the GDPR, they are personal data. The EU Charter of Fundamental Rights (CFR) states that everyone has the "right to the protection of personal data" Article 8 (1) CFR. More specifically, it defines how this data must be handled and what rights the affected person wrt. personal data (Article 8 (2) CFR). The ePrivacy Directive 2002/58/EC (amended in 2009), specifies this in more detail in relation to privacy and electronic communications. Article 5 deals with the "Confidentiality of the communications". The conditions under which storage is permissible are therefore both a question of whether the user is informed and whether he or she gave his or her consent. However, the article excludes purely technical cookies if they are necessary for the transmission of a message or are seen as "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service". Excluding technically necessary cookies, the directive raises the question of what a legally admissible cookie disclaimer should look like. According to Recital 25, users must be provided with "clear and precise information". They should be informed about exactly what data is stored. Furthermore, they should have the opportunity to disagree to the storage of their data. The Recital and the Article itself thereby refers to the prior existing Data Protection Directive superseded by the GDPR. The latter defines that consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes"(Article 4 (11) GDPR)[21].

2.1 Opt-In and Opt-Out

In the course of this definition, the question arises, as to what voluntariness should look like, especially since Recital 25 of the ePrivacy Directive mentions that "requesting consent should be made as user-friendly as possible". Two types of cookie disclaimers occur. Those with an opt-in version, in which the user gives his consent for individual cookie types by checking a box, and the opt-out variant in which the user disagrees with the use by removing check marks in boxes checked before. For example, the user could be asked to agree to five evaluation procedures of his data by actively setting check marks (Opt-In) in these individual cases the procedure may require additional work or simply to move on quickly with a click on "Consent" if the check marks have already been set, instead of deactivating the set check marks again individually (Opt-Out). Courts decided in this regard, such as the European Court of Justice in 2019, that it was not "validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent" [4]. In this context, the court also ruled on the issue of whether there is a difference for personal and non-personal data. According to the ruling, the regulation should not be "interpreted differently" in this regard. It was also decided that information regarding the duration of the cookies' function and their transfer to third parties must be communicated to the user.

The discussion about the pre-ticked boxes also arose in connection with the implementation of the Directive into German law. Because the ePrivacy Directive is not a directly applicable law in the member states, it must be implemented in national law. Contrary to what many had previously assumed, the German Feder Court of Justice ruled in May 2020 that the wording in the already existing Telemediengesetz (TMG), which does not require an opt-in version, could be cured for the time being by a broad interpretation that conforms to the Directive (German Federal Court of Justice, 2020) [8]. The German government is therefore adapting the wording in the new Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG), which replaces the TMG in some respects, including the question of data protection provisions for Telemedia, and will come into force in December 2021. The TTDSG provides for a provision in §24 TTDSG that is very close to the wording of the ePrivacy Regulation and places consent in conjunction with the GDPR principles of freedom and clear information.

Still pending is the new ePrivacy Regulation, which has been in the works for a long time and supersedes the ePrivacy Directive. Unlike the Directive, as it will be a Regulation, it would then no longer have to be implemented in national law and would thus also replace the TMG or the TTDSG in Germany regarding cookies. Since it is considered a supplement to the GDPR, it should also have come into force with it. However, there are only drafts so far. The European Council under the Portuguese Presidency published a statement on February 10, 2021, in which an agreement was announced within the Council [19]. Regarding cookies, the press release mentions once again that users should have a "genuine choice on whether to accept cookies or similar identifiers". In addition, in contrast to the previous provisional version of the ePrivacy Regulation, the possibility of a paid alternative of the website with the help of a paywall is addressed.

2.2 Territorial Scope

The coming ePrivacy Regulation is designed as a supplement to the Data Protection Directive (Article 1(II)). As the latter has been superseded by the GDPR, as mentioned before, the ePrivacy Regulation is also subject to the territorial scope of the GDPR. Article 3 provides four alternatives as to how it applies.

1) The GDPR applies when the processing of personal data is carried out by an establishment in the Union. It does not matter where the processing takes place and whether it is only an effective or an actual practice of the activity.

2) According to paragraph two, it is also sufficient if the processors, even if they are not established in the Union, specifically offer their goods and services to data subjects within the Union. It is not decisive whether they do so for free or for payment. The question of when a processor offers its services in the targeted manner is described in more detail in Recital 23. According to this, mere accessibility is not sufficient. The use of a language or currency that is customary in the Union, however, is.

3) In the same paragraph, another possibility of applicability is described, which is particularly important in connection with cookies. To the extent that the processing of the data is related to "the monitoring of their behavior as far as their behavior takes place within the Union", the GDPR is also applicable. In this regard, according to Recital 24, the decisive factor is whether persons are "tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes". Thus, the use of cookies is also covered by this paragraph and the GDPR applies if the storage of cookies is intended to create a profile.

4) Finally, the GDPR is also applicable if the law of a Member State of the European Union is applicable at the location of the processor due to international law provisions.

2.3 Summary

In summary, we therefore find that websites that store data of users within EU in the form of cookies should have cookie disclaimers that meet at least the following requirements to be GDPR compliant: (1) They must inform the user in a clear and concise manner what data they are storing, for how long they are going to be used and whether they are given to third parties. (2) The cookie disclaimer must give the user the option to decline the storage of data. If cookies are to be used, the user has to actively accept each type of cookie. Opt-Out designs are not permitted. Before that, no data may be stored (except necessary ones). (3) The storage of technically necessary cookies is excluded from the given definition. These do not require any notification and thus no active rejection. It is important to note that these are only minimum requirements, which have been confirmed by court decisions.

3 RELATED WORK

We describe the previous research on the topic of cookie disclaimers, namely, the research on legal requirements, studies proposing classifications of cookie disclaimers and further examinations of the cookie disclaimers.

3.1 Minimum legal requirements and possible violations of existing European law

The question which legal requirements cookie disclaimers must fulfill has already been addressed in several scientific papers. The selection of legal requirements shows overlaps but is never congruent. This shows that it is not clear which requirements really have to be met for a legal cookie disclaimer. Cristiana Santos, Nataliia Bielova and Célestin Matte established in 2020 22 legal requirements [20]. They refer to the ePrivacy Directive and the GDPR. It is particularly interesting to note their statement that it is practically impossible to fulfill all the requirements due to the "current architecture of the web" and due to the lack of standards (p. 1).

In a related approach, potential violations of existing law are classified. In another paper, the same researchers Célestin Matte, Nataliia Bielova and Célestin Matte have identified potential violations of existing European law [17]. In the study, they refer to cookie banners provided by content management providers (CMPs). The Interactive Advertising Bureau Europe (IAB Europe) has developed the Transparency and Consent Framework (TCF), which covers practices of "actors of the tracking and advertisement industry regarding consent collection" (p. 1), the CMPs. Matte et al. analyzed 1426 European websites using cookie banners developed by CMPs. Four possible violations were defined: "Consent stored before choice, no way to opt out, pre-selected choices, non-respect of choice" (p. 2). Thus, not only the cookie disclaimers were examined, but also the stored cookies. Among the sites examined by the authors, 54% of the websites were found to be non-compliant or to have at least one of the violations (p. 9). The study examines the implementation of the banners, which makes it more technical in nature compared to this paper. As a result of the study, it was also possible to develop a browser extension ("Cookie Glasses") that checks for violations.

Nouwens et al. are also investigating the CMPs [18]. The disclaimers are checked for their design, the occurrence of non- compliant elements and how much the banners meet the requirement of a "freely given" consent. The number of clicks needed to agree or disagree to the storage of the data is compared. The 10,000 most popular websites in the United Kingdom are taken into account. The British study also sets criteria that cookie disclaimers must meet to be legal: "consent must be explicit, accepting all is as easy as rejecting all (clicks), no pre-ticked box". According to the study, only 11.8% of the websites examined meet the minimal criteria set (p. 5).

3.2 Cookie disclaimer classification

The formation of categories, which is a large part of this work, has also already been dealt with in various ways. In "We Value Your Privacy... Now Take Some Cookies", Degeling et al. look at the most popular websites in 28 EU member states [7]. Primarily, they examine how privacy policies change over time on the different websites. To do this, they observed the privacy policies of the top 500 websites for each of the countries from December 2017 to October 2018. Part of the study also included categorizing the realization of consent for cookies, dividing 28 typical banners into seven categories: No Option, Confirmation, Binary, Slider, Checkbox, Vendor and Other (pp. 8-9).

Kulyk et al. have also created categories for cookie disclaimers based on the content of the messages [13]. The five groups refer to the information given about what the cookies are used for.

Classifications of cookie disclaimers have also been made in terms of design. When investigating dark patterns, describing "instances where designers use their knowledge of human behavior (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest" [10], Gray et al. made a distinction across various criteria in 2021 [11]. They differentiate between "initial framing" and "configuration and acceptance" and refer to a total of four design decisions that can be made. All decisions are treated from four perspectives: designer, interface, user, and social context.

A recent study by Kampanos and Shahandashti examined 17,000 cookie disclaimers and the cookies stored on Greek and UK websites on a large scale [12]. The disclaimers were distinguished by the wording of their options (Affirmative, Negative, Informational and Managerial) in all 16 possible combinations and the number of options that were displayed. The analyses showed that less than half of the sites comply with the existing laws at all. Most sites additionally use nudging to get users to choose the privacy-unfriendly options through positive language and selection of options. The decrease in the proportion of disclaimers counted compared to older similar studies was explained by the high number and thus the included not so popular websites.

3.3 Further studies

The approach by Carpineto, Re and Romano examined the top 500 country-specific websites for Italy as well as Italian Public Administration websites [3]. The authors analyzed the relationship with their CooLCheck tool between the query for "tracking cookie" and their actual storage and usage. However, the design of the individual cookie dialogues was not considered at all.

Leenes and Kosta also examined 100 exemplary websites regarding their cookie disclaimers during their study on the question of how existing European law has been implemented in the Netherlands [15]. These were the top 100 websites in the Netherlands. They examined whether a cookie disclaimer was present and also which cookie disclaimers were examined. They concluded that "there is significant variance in the way websites treat cookies and consent and that from a cursory inspection it is difficult to tell whether the sites comply with the regulation".

Travisan, Traverso, Bassi and Mellia also examine the status of implementation of the legal requirements in Europe [22]. For this purpose, they examine cookie notifications for 25 countries (21 member states and four other non-EU countries) in each of 25 categories of each of the 100 most popular websites. The question is asked whether cookies are already stored before consent is given. The

result shows that 49% of the websites examined do not adhere to the requirements of the ePrivacy Directive (p. 127).

The relevance of the user's country in relation to the cookie disclaimers displayed was shown in a 2019 study by Van Eijk, Asghari, Winter and Narayanan [24]. The results showed that the differences in disclaimers are mainly due to their top level domain (TLD) rather than the country from which the page is accessed. One exception is the .com TLD, where the decisive factor is in particular whether the website is accessed within or outside the EU.

4 INVESTIGATION OF POPULAR WEBSITES

We take the following five-steps-approach to analyze the top 500 Alexa websites for Germany: (1) Identification of categories of cookie disclaimers based on disclaimers from a sample of 100 websites. (2) Categorizing the cookie disclaimers of the Alexa 500 most popular websites in Germany. Those disclaimers that could not be assigned to one of the categories identified in step 1 were put aside for a third step. (3) Identifying categories from those disclaimers which we put aside in step 2. (4) Judging the categories from a legal point of view. (5) Categorizing 500 cookie disclaimers using these additional categories.

4.1 Alexa top websites

In order to carry out our research, websites had to be selected that served to create the categories on the one hand and to evaluate them on the other. Amazon's Alexa Top Websites service was used as the basis for this paper, similar to some of the other studies on the topic [3, 18]. Alexa Top Sites is a tool by Alexa Internet, a web analytics service offered by Amazon. According to its own information, a browser extension collects data via a traffic panel, which is summarized into a "Global Traffic Rank". This measures how websites compare with each other. The company specifies on its website: "The rank is calculated using a proprietary methodology that combines a site's estimated average of daily unique visitors and its estimated number of pageviews over the past 3 months" [1]. Alexa's traffic rank is determined every day according to its own information. It is composed of the "unique visitors", i.e., the number of individual users who call up a page on a given day, and the "pageviews", i.e., the total number of times a URL is called up. For the latter, calls by the same user on one day are counted as a single call. In addition, "data normalization" is performed, but is not described in more detail. For the called domains, subpages and subdomains are not counted individually. Exceptions are those for blogs, for example, which can be identified automatically. The company mentions that only the first 100,000 ranks would be listed, because the data collection, which is based on the data of registered Alexa users, is too small for further ranks [1]. In addition to the global figures, a country-specific ranking is offered, which is determined using the same scheme. The company does not provide more detailed information on how this rank is calculated.

4.2 Identification of the categories using a sample of 100 websites

In a first step, exemplary 100 websites were examined: Top 1-25; 101-125; 201-225; 401-425. Thereby, we excluded a potential effect that the type of cookie disclaimers correlates with the "Alexa Traffic Rank". These 100 were taken from the top 500 Alexa websites on November 17th 2020 [1]. With the help of an automated tool, screenshots of the websites were created. The screenshots are taken from the desktop versions of the websites. They were created on a Linux operating system in a Chromium browser with a German IP address, where all cookies were deleted beforehand. The study was limited to websites that were available in German or English at the time of the study. This enabled the cookie disclaimer to be identified, read, and understood. Thus, 17 had to be excluded due to language issues and one because they was not available. If websites from the same provider appeared several times with different top-level domains, these were also included several times in the analysis. The search engine "Google" is particularly conspicuous here, appearing twice in the top 10, once with "google.com" and once with "google.de". In summary, the cookie disclaimers of 18 websites from the sample were not examined.

The screenshots were categories and the categories were discussed between two of the authors to agree on a list of categories identified during this step: Five categories of cookie disclaimers were identified. Two of these categories also had alternative forms in which it appeared in the sample. Thus, there are in total nine categories. Note, the identified nine categories refer to the two conditions described above: Informing the user and the possibility of limiting the storage of his data. Additionally, the design is used for the distinction.

In the following, the identified categories are described in more detail, so that they can be used in the next step for the classification of all top 500 Alexa websites:

0. No disclaimer. This includes websites that do not display any cookie disclaimer.

1. "Accept all" (and "Leave page"). The disclaimer has one option[1] that allows to accept all cookies. No possibility exists to limit this consent. This category includes those disclaimers that also provide a "leave page" option that allows website visitors to leave the website (if they do not want to accept the cookie settings). Note, some may be more precise about the type of cookies and others just talk about cookies in general.

2. "Accept all" and "More information". All cookies can be accepted with one click. It is not possible to limit this consent. Furthermore, the user can get more information[2] (e.g. on the cookies or privacy policies in general) via a second option to be clicked on in the disclaimer. Either you can get the "More information" easily through a well visible link or button, or the link can be embedded and almost hidden in the text. For this category, there is no differentiation made – for this paper – regarding the design and placement of the options. Note, some cookie disclaimers in category 2 provide a way to limit the consent, if visitors pay a fee (i.e., an option is given to turn off cookies for advertising purposes and, in some cases, tracking cookies by paying a fee).

[1]Note, the following labels occurred for the "Accept All" option, among others: "I agree", "Select All", "Ok, understood", "Activate All", "Agree", "Accept Cookies".
[2]The following designations occurred for the "More information" option: "Privacy policy", "Cookie policy", "More info", "More details", "Privacy statement", among others.

3. "Accept all" and config options on second page. Two options are offered to deal with the cookie disclaimer. On the one hand, the cookies can all be accepted with one click (note, different phrasing exist for this option). On the other hand, there is the possibility to proceed to a second page with more options[3] incl. to only accept some cookies. The possibility to reach this second page can be announced in different ways (e.g. in the text, via a link, or on a button). It doesn't matter which word are used, as long as one can change the settings there. Note, to reject some cookie types it is needed to visit this second page.

There are two dimensions to be considered for this category. The *first* dimension describes whether an option is highlighted. The option "Accept all" can be specially highlighted[4] (I), or the two options are displayed equally (II). An option is considered to be specially highlighted if either of the following two cases holds: [case1] It is provided as a button and the other option is presented as link-text; [case2] both options are provided as buttons but the highlighted option is the only one with a colored background. Also, if the possibility of further options is presented in a link and not in a button, unlike the possibility of "Accept all", the latter is considered highlighted. The *second* dimension describes whether opt-in or opt-out with respect to the types of cookies being selected on the second page is implemented. In the opt-in subcategory (A), all options (except technically necessary cookies) are not yet selected. In the opt-out subcategory (B) , in contrast, all options (being more than just technically necessary cookies) are already selected.

Thus there are actually four different categories 3.A.I, 3.A.II, 3.B.I, and 3.B.II. Note, some of the disclaimers may also contain an option of accessing more information, such as the privacy statement. However, this is not used to further distinguish between subcategories.

4. "Accept all" and config options on the disclaimer. In this case, the options to change the cookie setting is integrated on the main disclaimer. Furthermore, a list of cookie types is provided. There are two options on the disclaimer while the accept-all-option is the highlighted one[5]. Thus, the user can either accept all cookies with one click or accept the selected cookie categories (while users could have changed the selected cookies before accepting them). Here, we distinguish two subcategories: The opt-in variant applies for the subcategory 4.A, which means that only the technically necessary cookies are selected in the option. This option can be selected by clicking a button with a title like "Save options". It differs from the subcategory 4.B, where all options are selected at the beginning.

Note, we made the following assumption: The accept-all option means that website visitors agree to store cookies beyond the technically necessary cookies. A verification of this claim is to be done in a future work.

[3]For "Options", for example, the alternative phrases "Configure", "Customize settings", "Manage cookies", "Change cookie settings", "Personalize" and "More options" occurred.
[4]Note, in theory, also the other option could be highlighted, but in the examined websites, this case was not included. Consequently it is also not identified as a (sub)category.
[5]Note, in theory, it could be that none of the two options is highlighted or that the privacy-friendly option is highlighted. However, this did not exist in the examined websites.

4.3 Classifying the 500 most popular websites

After the 100 exemplary websites, the next step was to look at the remaining 400 of the 500 most popular websites in Germany. Note, in total, it was not possible to examine 111 websites, either because they were not available in German or English or because they were not accessible. This left us with in total 389 websites and their cookie disclaimers to be classified into the described nine categories.

352 of the cookie disclaimers corresponded to the defined nine categories and were classified into them. The remaining 36 cookie disclaimers were considered separately as they did not match to one of the nine categories. We identified categories for these 36 disclaimers. Again, categories were proposed and discussed between two of the authors. As a result the nine categories from step-1 were extended by four additional ones, namely 4.A.II, 4.B.II, 5.I, 5.II. The final categorization was carried out independently by two of the authors.

The additional categories are described in the following paragraphs:

4. Extended to 4.A.I/II and 4.B.I/II. : It was needed to introduce both dimensions from category 3 also for category 4, i.e. instead of only considering 4.A (opt-in, accept-all highlighted) and 4.B (opt-out, accept-all highlighted), we also found a few in which not the accept-all option was highlighted. Thus 4.A became 4.A.I and 4.B became 4.B.I. Furthermore, 4.A.II and 4.B.II was added as categories to reflect cases in which both options are displayed in the same way.

5."Accept all"and "Refuse" + config 2nd page. : This category always includes "Accept all" and "Refuse" with a single click and can – but does not have to – offer the option of changing individual cookie settings on a second page (other than technically necessary cookies, which are relevant for the website to function[6]) Note, the options for refusing the cookies can also be embedded in the text (or even hidden in the text). For this category it is only important that the refuse-option is there. Furthermore, we decided to treat agreeing to technically necessary cookies in the same way as rejecting all. This possibility is again titled with different names, for example, "Reject cookies", "Disagree", "Deny", "Reject all". We distinguish between 5.I and 5.II depending on whether the accept-all option is highlighted (I) or whether both options (reject-all and accept-all) are displayed in the same way.

Examples of disclaimers from the resulting five main categories (excluding category 0 with no disclaimer shown) are provided in Figures 1 to 5.

Fig. 1. Category 1 (source: rapidgator.net, Nov. 17th 2020).

4.4 Data protection and privacy implications

The following is a legal classification of each category. The information about the type of data stored, the possibility of separate selection, the distinction between an opt-in and an opt-out option,

[6]Note, we assume that this action is an objection to the collection and storage of cookies that are not technically necessary, but leave it for future work to check whether our assumption is correct.

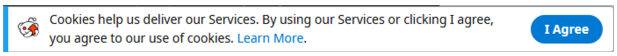

Fig. 2. Category 2 (source: reddit.com, Nov. 17th 2020), as website visitors can get more information (using the Learn-More link).

Fig. 3. Category 3.A.I (source: amazon.de, Nov. 17th 2020), as the accept all option is highlighted and due to the fact that the disclaimer is opt-in on the second / "settings" page - which is not displayed here due to space reasons.

Fig. 4. Category 4 (source: hornbach.de, Nov. 17th 2020). The subcategory of the shown disclaimer is 4.A.I

Fig. 5. Category 5 (source: rewe.de, Nov. 17th 2020). The subcategory of the shown disclaimer is 5.II

and the user-friendliness are used to decide whether a disclaimer is privacy-friendly or not, according to the given definition. Once again, it should be mentioned that it is not yet investigated what kind of cookies are collected. In addition, aspects regarding the design or the exact form of presentation are not included here, but they can have an impact on the assessment of privacy friendliness.

0. Since no cookie disclaimer exists, the user can neither be informed nor given the possibility to disagree with the storage of his data. Thus, the website violates existing law and is not privacy friendly if and only if they store more than just technical necessary cookies.

1 and 2. It is necessary according to the ePrivacy Regulation to provide information about cookies. However, this is only the case of category 2 ('Accept all' + more info) but not for category 1. Additionally, the user must have the ability to agree or disagree with each cookie type (other than technically necessary cookies). Disagreeing is not possible in both categories. This cookie disclaimer therefore violates – from our point of view – existing law if more than just technically necessary cookies are stored. Note, some cookie disclaimers in category 2 provide a way to limit the consent, if visitors pay a fee. As there is a way to limit consent, it would not – at least not obviously – violate existing law.

3. (i.e. 'Accept all' + refuse on 2nd page) So far, due to our knowledge, there have been no rulings in Germany which would allow to generalize on the question of whether certain buttons may be specially highlighted. Thus, for now, there is no legal difference between the subcategories I and II. The question of the opt-in and opt-out option, on the other hand, has been clarified by the courts. Thus, the subcategories 3.A.II with an opt-in option is clearly compliant with the law, 3.A.I could be as well – as long courts have not been requested and judged on highlighting and/or the fact that it takes more effort to reject then to accept cookies. However, the subcategories 3.B.I and 3.B.II with the opt-out option are not compliant with existing laws, if more than technically necessary cookies are stored.

4. Since the subcategories 4.B.I and 4.B.II display an opt-out option, according to existing court rulings, the disclaimers in these categories are not compliant with the law, if more than technically necessary cookies are stored. The disclaimers in 4.A.II categories, however, are compliant: Information is given about what data is stored and the user can decide for each cookie type with an opt-in option whether to agree to it or not. 4.A.I could be as well for the above mentioned missing ruling on the highlighted options.

5. This main category is likely to fulfill the requirement for providing information for collection and storage. In addition, it provides the ability to easily reject cookies other than the technically necessary cookies. Category 5.II fulfills – from our point of view – the legal requirements. For the same reason as above for category 3 and 4, 5.I could fulfill as well.

4.5 Website assignment

The evaluation of the frequencies (see Table 1 showed that, as the *most frequent* category, around a third of the 389 investigated websites (134 total, 34.4%) did not display a cookie disclaimer. This category, however, was less prevalent among the websites in top 100 websites than in the ones in positions 101-500 (17 of 76, i.e. 22.4% compared to 117 of 313, i.e. 37.4% frequency). The *second most frequent* category (108 total, 27.8%) was 3.A.I, namely disclaimers with a highlighted "Accept All" button and the setting option that refers to a second page where the user can select the cookie types by means of an opt-in. This category was more frequent for websites in top-100 (36.8% frequency) than among the rest of the websites (25.6% frequency). In the *third place*, we find category-2 (69 total, 17.7%; 21.1% among the websites in top 100, 16.9% on websites in 101-500): there is an "Accept All" button and a reference to more information, for example the privacy policy. Note, five of these 69 cookie disclaimer contained the option to limit the cookies if users

pay a fee. Category 5.I is found in *fourth place* with 21 websites (6.6% in top 100, 5.1% in 101-500). On the first page, there is the option to accept only the technically necessary cookies and reject the rest with only one click. However, the "Accept All" button is highlighted.

Table 1. Occurrence of the categories at the examined websites. It denotes categories that are compliant but highlight the "Accept all" button, it denotes categories that are compliant and do not highlight any button. The rest of categories would be compliant only if just the necessary cookies are collected by the website.

	1-500	1-100	101-500
0 no disclaimer	134	17	117
1 only 'accept all'	5	0	5
2 'accept all'+ more info	69	16	53
3.A.I 'accept all'+opt-in on 2nd p. I	108	28	80
3.A.II 'accept all'+opt-in on 2nd p. II	14	4	10
3.B.I 'accept all'+opt-out on 2nd p. I 'accept all'+opt-out on 2nd p. I	16	5	11
3.B.II 'accept all'+opt-out on 2nd p. II	2	0	2
4.A.I 'accept all'+opt-in on discl. I	9	1	8
4.A.II 'accept all'+opt-in on discl. II	2	0	2
4.B.I 'accept all'+opt-out discl. I	1	0	1
4.B.II 'accept all'+opt-out discl. II	1	0	1
5.I refuse with one click/config 2nd p. I	21	5	16
5.II refuse with one click/config 2nd p. II	7	0	7
Total	389	76	313

There are in total 69 out of the 389 investigated websites (=5+64[7])/ 17.7% websites that would not be compliant to legal regulations because cookies cannot be rejected, assuming that more than only technically necessary cookies are stored (categories 1 and 2). 181 (=108+14+16+2+9+2+1+1+21+7; categories 3, 4 and 5) websites show a cookie disclaimer with the option to reject cookies (without payment). Out these 181 there are in total 142 (=108+14+16+2+1+1) / 78.5% websites that require at least one more click for rejecting cookies that are not technically necessary compared to the one click to accept all (categories 3.A+B.I+II, 4.B.I+II). There are 20 (=16+2+1+1) / 11.1% that implement opt-out although it violates existing law (categories 3.B.I+II, 4.B.I+II). There are in total 155 (=108+16+9+1+21) / 85.6% websites nudging their visitors into selecting accept-all option as this is the highlighted option (categories 3.A+B.I, 4.A+B.I, 5.I), and 9(=2+7)/ 4.97% that do not use any kind of nudging, making it possible for the website visitors to reject cookies with just one click without highlighting the "Accept-all" option (categories 4.A.II and 5.II). Thus, from the 181 websites showing a cookie disclaimer and providing an option to reject cookies, only 4.97% websites don't nudge their visitors into selecting accept-all.

[7]69 minus the five which have the option to limit the cookies if users pay.

4.6 Privacy implication assessment based on related work

The distinction between how many clicks one would require to change the cookie settings (that is, the main difference between our main categories 3, 4 and 5) has been investigated by Nouwens et al. [18], showing that consent for data use increases when the "Reject-all" button is not present on the first page. Utz et al. furthermore investigated the visual design of the disclaimers, showing that presenting the "Accept-all" option as a highlighted button increased the acceptance rate compared to presenting the option as a text link [23], confirming our intuition that disclaimers in subcategory II (that is, categories 3.A/B.II, 4.A/B.II, 5.II) are more privacy-friendly than the ones in subcategory I (categories 3.A/B.I, 4.A/B.I and 5.I correspondingly). This is also the case in a study by Machuletz and Böhme, showing that a highlighted default button leads to higher acceptance rate [16]. In contrast, a study by Grass et al. [9] found that dark patterns did not significantly increase (+ 3.95%) an already very high approval rate for cookie disclaimers (93.84%), including by highlighting the default button in color. Giving these results and the fact that nudging is broadly used, there is a need for further legal regulations.

5 DISCUSSION AND CONCLUSION

In the course of this research, a number of findings emerged regarding the privacy and data protection standard of cookie disclaimers on websites visited from Germany. For example, it was found that among the investigated websites that displayed a cookie disclaimer, only 21.5% (39 out of 181 websites, those in category 4AI/II and in 5I/II) allowed to reject cookies using *the same number of clicks* that would be required to accept them. Out of these 39 websites, the majority (30 websites, 76.9%) uses some form of visual nudging leading the user towards consenting to more extensive data collection. In total 85.6% of the investigated websites providing a cookie disclaimer with the option to reject cookies are visually nudging users towards accepting all cookies. Thus, our findings show the prevalence of dark patterns.

Hence, further investigation into how these dark patterns affect the users' decisions, as well as how the users can be protected from the dark patterns, are needed. In particular, the results of our investigation show the need to develop measures to support the user in protecting their privacy in wide-spread presence of dark patterns. Such measures would include a combination of awareness raising (e.g. warning the users that selecting highlighted option, or the option that is most easy to access, can have negative effect on their privacy) as well as providing actionable guidelines, such as using browser settings (e.g. incognito mode or settings that block third-party cookies) or third-party plugins that limit web tracking. On the other hand, one should avoid placing the total of responsibility on the end user, as the decision fatigue in having to interact with a

number of websites and their cookie disclaimers on a daily basis (see e.g. Kulyk et al. [13, 14]) could limit the extent to which the users would be able to pay attention to every disclaimer. Other stakeholders would therefore need to be involved, such as developers, in particular regarding their choices in the design of the disclaimers, policy makers who would be able to propose and enforce legislative measures to limit the use of dark patterns, as well as consumer agencies and data protection agencies to get more clarity about patterns violating the GDPR. In particular for the policy makers, we see a need to define more clearly which cookies can be classified and called 'technical necessary'.

ACKNOWLEDGMENTS

This research was supported by the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS).

The project was funded by the ministry of Science, Research and the Arts Baden-Württemberg as part of the DIGILOG@BW - joint research project with funds from the digilog@bw State Digitization Strategy.

We also want to thank Franz Lehr from TU Dresden (Germany) for the fruitful discussions on the legal aspects.

REFERENCES

[1] Inc.1996 2021 Alexa Internet. 2021. Alexa - Top Sites in Germany. https://www.alexa.com/topsites/countries/DE,retrieved from November 17, 2020.

[2] Claude-Etienne Armingaud and Lucile Rolinet. 2020. French Data Protection: French Supervisory Authority Publishes Updated Guidance on Cookie and Other Tracking Technologies. The National Law Review: https://www.natlawreview.com/article/french-data-protection-french-supervisory-authority-publishes-updated-guidance, last accessed on 25.02.2021.

[3] Caudio Carpineto, Davide Lo Re, and Giovanni Romano. 2016. Automatic Assessment of Website Compliance to the European Cookie Law with CooLCheck. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* (Vienna, Austria) *(WPES '16)*. Association for Computing Machinery, New York, NY, USA, 135–138. https://doi.org/10.1145/2994620.2994622

[4] Court of Justice of the European Union. 2019. Judgement of the court (grand chamer), case C-673/17, Planet49.

[5] Court of Justice of the European Union. 2020. PRESS RELEASE No 125/19. Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet49 GmbH. https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf, last accessed on 25.02.2021.

[6] Danish Data Protection Authority. 2017. Nye retningslinjer om behandling af personoplysninger om hjemmesidebesøgende. https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/feb/nye-retningslinjer-om-behandling-af-personoplysninger-om-hjemmesidebesoegende/, last accessed on 3.10.2020.

[7] 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. *Proceedings 2019 Network and Distributed System Security Symposium* (2019). https://doi.org/10.14722/ndss.2019.23378

[8] German Federal Court of Justice. 2020. IZR 673/16, Cookie-Einwilligung II.

[9] 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 (2021), 1–38.

[10] 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

[11] 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. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (May 2021), 1–18. https://doi.org/10.1145/3411764.3445779

[12] Georgios Kampanos and Siamak F Shahandashti. 2021. Accept All: The Landscape of Cookie Banners in Greece and the UK. *arXiv preprint arXiv:2104.05750* (2021), 213–227.

[13] Oksana Kulyk, Nina Gerber, Annika Hilt, and Melanie Volkamer. 2018. "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. In *3rd European Workshop on Usable Security (EuroUSEC), London, England, April 23, 2018*. Internet Societa, Reston 8VY).

[14] Oksana Kulyk, Nina Gerber, Annika Hilt, and Melanie Volkamer. 2020. Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity* 6, 1 (2020), tyaa022.

[15] Ronald Leenes and Eleni Kosta. 2015. Taming the cookie monster with dutch law–a tale of regulatory failure. *Computer Law & Security Review* 31, 3 (2015), 317–335.

[16] 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.

[17] 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. (2020), 791–809.

[18] 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. *arXiv preprint arXiv:2001.02479* (2020).

[19] Council of the EU. 2021. Confidentiality of electronic communications: Council agrees its position on ePrivacy rules. https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/,retrieved from February 26, 2021.

[20] Cristiana Santos, Nataliia Bielova, and Célestin Matte. 2020. Are cookie banners indeed compliant with the law? *Technology and Regulation* (2020), 91–135.

[21] The European Parliament and of the Council of European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj, last accessed on 25.02.2021.

[22] Martino Trevisan, Stefano Traverso, Eleonora Bassi, and Marco Mellia. 2019. 4 years of EU cookie law: Results and lessons learned. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (2019), 126–145.

[23] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (Nov 2019), 973–990. https://doi.org/10.1145/3319535.3354212

[24] Rob Van Eijk, Hadi Asghari, Philipp Winter, and Arvind Narayanan. 2019. The impact of user location on cookie notices (inside and outside of the European Union). In *Workshop on Technology and Consumer Protection (ConPro'19). IEEE*. IEEE, United States, 6.