This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices

CARLOS BERMEJO FERNANDEZ, Hong Kong University of Science and Technology, Hong Kong, SAR
DIMITRIS CHATZOPOULOS, Hong Kong University of Science and Technology, Hong Kong, SAR
DIMITRIOS PAPADOPOULOS, Hong Kong University of Science and Technology, Hong Kong, SAR
PAN HUI, Hong Kong University of Science and Technology, University of Helsinki, Hong Kong, SAR, Finland

Data protection regulatory policies, such as the European Union's General Data Protection Regulation (GDPR), force website operators to request users' consent before collecting any personal information revealed through their web browsing. Website operators, motivated by the potential value of the collected personal data, employ various methods when designing consent notices (e.g., dark patterns) in order to convince users to allow the collection of as much of their personal data as possible. In this paper, we design and conduct a user study where 1100 MTurk workers interact with eight different designs of cookie consent notices. We show that the nudging designs used in the different cookie consent notices have a large effect on the choices user make. Our results show that color-based nudging bars can significantly impact the participants' decisions to change the default cookie settings, despite using dark patterns. Also, in contrast to previous works, we report that users who do not use ad-blocking software are less likely to modify default cookie settings. Our findings demonstrate the importance of nudged interfaces and the effects orthogonal nudging techniques can have on users' choices.

CCS Concepts: • **Human-centered computing** → **User studies**; *Web-based interaction*; • **Security and privacy** → *Usability in security and privacy*.

Additional Key Words and Phrases: cookies, nudging, interactions, behaviour

ACM Reference Format:
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 (October 2021), 22 pages. https://doi.org/10.1145/3476087

1 INTRODUCTION

The General Data Protection Regulation (GDPR)[1], which is in force in Europe since May 2018, requires website operators to have a legal basis for collecting and processing personal data. Websites use cookies to track information that is related to users' browsing activity. Example uses of the collected data are user profiling and targeted advertising [17]. The GDPR forces website operators to inform users, using cookie consent notices, about the data they collect during their browsing

[1] https://data.europa.eu/eli/reg/2016/679/2016-05-04

Authors' addresses: Carlos Bermejo Fernandez, Hong Kong University of Science and Technology, Hong Kong, SAR; Dimitris Chatzopoulos, Hong Kong University of Science and Technology, Hong Kong, SAR; Dimitrios Papadopoulos, Hong Kong University of Science and Technology, Hong Kong, SAR; Pan Hui, Hong Kong University of Science and Technology,, University of Helsinki, Hong Kong, SAR, Finland.

2573-0142/2021/10-ART346 $15.00
https://doi.org/10.1145/3476087

Term	Description
Nudging	Soft-paternalism towards more privacy-aware settings in the users' decision-making process. Nudging techniques are tactics that designers may use to help users in making more informed decisions
Dark patterns	Practices such as interface design that influence individuals to make decisions in favor of data collectors (e.g., accept the default cookie consent so websites can collect more information about visitors)

Table 1. Description of our used terminology (following similar definitions from [1, 19]).

and give them the option to select the types of data they are willing to allow website operators to collect. The GDPR affects any website that collects or processes personal data of EU citizens or hosts the collection or processing in the European Union [18].

However, it is common practice for website operators to ensure consent using interface design "tricks" like *dark patterns* that influence users towards accepting the default selection. *Dark patterns* usually allow website operators to collect anything they have tools for [32, 36]. For example, one such technique can omit the *decline cookies* button to influence acceptance consent. Likewise, cookie consent notices seldom display the cookie settings on the first screen. At the same time, some design approaches use a highlighted "Select all and confirm/accept" button that steers users towards allowing website operators to collect all possible information [29, 36, 46]. Machuletz *et al.* [29] examine"*How do users react to design features of multi-purpose consent dialogues on the web in terms of actual behaviour and stated perceptions?*" Their experimental results confirm, in alignment with previous work [36, 46], those design elements, such as the highlighted button to select all cookie purposes, do affect users' responses.

Another technique that website designers widely use in order to influence users' decisions while browsing is *nudging* [2, 11, 43]. For example, in a cookie consent display, the "accept-essential-only" setting may be highlighted in color in order to nudge users towards a more privacy-aware choice. The utilization of nudging techniques in cookie consent notices certifies that users are not always aware of the possible risks of their choices and that these decisions can be affected by nuances in system design [2]. Regulations included in the GDPR can lead to scenarios where both dark patterns and nudging techniques are implemented in the same cookie notice since the GDPR does not limit website operators from designing their cookie notices in a way that influence users towards accepting the default settings [19, 36, 40]. Even in websites that are built to ensure compliance with GDPR, we can still find dark patterns that "bypass" the *GDPR-by-design* feature [40].

Although several studies, such as the ones from Utz *et al.* [46] and Nouwens *et al.* [36], examine a design space where both dark patterns and nudging techniques are used, these studies do not address popular real-world use cases such as the case with hidden cookie settings menu (e.g., under a button). As a result, the authors of these works do not analyze how dark patterns might affect the users' responses in the scenarios where users require additional effort to modify the default cookie settings. We further elaborate on the difference between this work and prior works in the area in the Related work and Discussion sections.

In this paper, we present the findings of a user study we conducted with 1,100 participants in Amazon MTurk[2] and eight different design combinations of cookie consent notices: four different nudging mechanisms (no nudging, bar, settings, bar and settings) combined with two dark pattern mechanisms (highlighted/non-highlighted accept-cookies button). Our study aims to find an answer

[2] www.mturk.com

to the following question: *"how do users react to nudged cookie consents?"* We initially examine the effects of nudging in the cookie consent notices on participants' responses. After that, we analyze features such as browser, screen size, and operating system that may impact participants' responses. In this paper, we use the term nudging to refer to subtle changes in the cookie consent design that guide users towards privacy-aware decisions [43]. Dark patterns, on the contrary, influence users to give away more information to data collectors (opt-out default settings in the cookie consent). See Table 1 for more detailed definitions of how we use these terms in this paper. As several works show [29, 46], despite current regulations to protect the privacy of individuals, data collectors are always one step ahead in making users share personal information (e.g., via dark patterns). The findings of this work highlight the potential of nudging for helping users make more informed decisions [11] about their privacy and the possibility that the proposed nudges can counterbalance current dark pattern techniques (e.g., highlighting the "accept" button). Our results show that dark patterns, when coexisting with nudging, do not significantly influence users to accept the default cookie settings.

We propose two nudging techniques motivated by previous works [16, 29]. The *first* technique displays the number of selectable cookies at once together with the cookie notice [29]. Motivated by a popular finding in the field of psychology, i.e., that a large number of options can have adverse effects on the users' decision-making process [14], we only show the four most common cookie types. The *second* technique builds on top of previous works [16, 52], where a color-based bar (e.g., green to red) visualizes the number of enabled cookies. Additionally, we evaluate the users' responses when these two nudging techniques are displayed with a common dark pattern technique: highlighting the accept button with green color. The second proposed nudging bar has stronger effects on participants' behaviour even when comparing it with the displays of selectable cookies evaluated in previous works [29, 36] and despite the longer time required to open the second display to customize the default cookie settings. Our results differ from findings in the work of Utz *et al.* [46], showing that users who do not use ad-blockers have a significantly lower tendency (less than 2%) to change the default cookie settings.

2 RELATED WORK

Before providing further details regarding the conducted user study, we discuss state-of-the-art procedures for presenting cookie consent notices, dark pattern design, and nudging techniques.

2.1 Cookie consent notices

Following the GDPR requirements, cookie consent notices require *explicit, informed, and withdrawable consent by users.*[3] The most common approach for requesting users' consent during web browsing is via checkboxes on web cookies [46]. Some cookie consent notices display a notification using a banner saying that the website uses cookies without additional functionalities [46]. Other notices display some functionality in the form of submit buttons, opt-in choices for each cookie purpose, submit/reject, or a combination of them [46]. However, current practices of cookie consents have been shown to be sub-optimal as they block the users' primary purpose, which is accessing the website [36, 40]. Furthermore, many cookie consent forms show long privacy policies [21], or use interface tricks to influence users into accepting the default cookie settings [12, 29, 36, 46]. Moreover, the opt-out settings of privacy policies in many websites are difficult to find or misleading [20]. These issues tend to habitually make users choose the "accept all" option in cookie dialogues [10]. As a result, cookie consent notices function more as informative notifications than actual mechanisms for users to control the information they are willing to share. Finally, Nouwens *et*

[3] https://gdpr.eu/cookies

al. [36] have proposed the idea of embedding cookie consent notices in browsers so that users do not have to reply in every notice.

2.2 Dark patterns

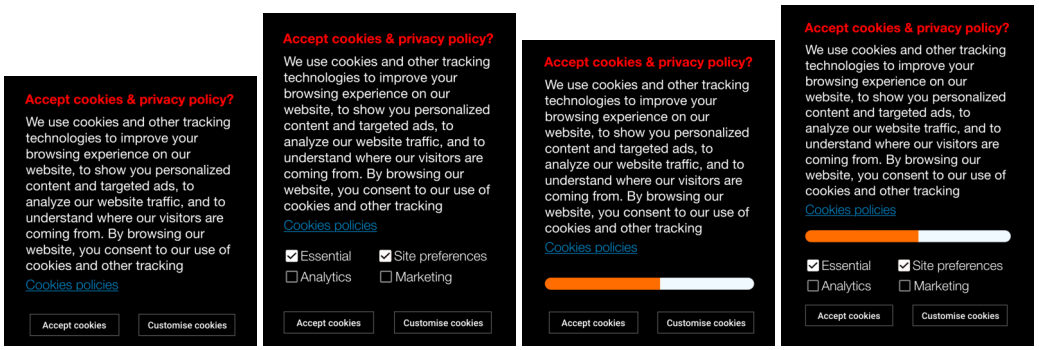
One of the most popular "tricks" used in the design of cookie consent windows in order to influence users towards accepting the default cookie selection is the use of so-called *dark patterns* [19]. These interface design tricks are usually not beneficial to individuals as the main goal is to deceive people even when consent is required. These practices have been openly reported by consumers,[4] and analyzed by researchers [29, 32, 36, 46]. Nouwens *et al.* [36], show that the lack of an opt-out button increases consent by 22%. Machuletz *et al.* [29] evaluate the effectiveness of dark patterns with a highlighted button "accept/submit all", where the results show that this increases users' consent in comparison with the default non-highlighted button. Utz *et al.* [46] show that the position of the cookie notice does not have an impact on users' interaction with the cookie. Moreover, the authors evaluate the use of binary choices (accept-reject), where users are more willing to accept the default cookie selection even when both buttons have the same design. The authors in [32] propose an automatic technique to study dark patterns in websites. The results from the automatic tool show that despite the current GDPR, websites still use dark patterns to trick users into accepting the preselected cookies to collect more information about them. Tools such as the one proposed by the authors of [32] can help regulators evaluate and score websites according to the interfaces used, improving users' privacy and the user experience with less deceiving interface designs.

2.3 Nudging

Nudging is any aspect of a choice architecture that alters the behaviour of the individuals towards more beneficial decisions for individuals [11, 43]. Nudging has been shown to be significant for improving users' privacy when used in the design of interfaces for smartphones [4, 6], and cookie consent notices [29, 36, 46]. Following the design space for nudging techniques proposed in [11], the authors of [29, 36] propose the visualization of opt-out cookie purposes in the consent notices. Similarly, in [36] the authors show that the display of the opt-out button (e.g., reject all) decreases users' consent by 8-20%. Machuletz *et al.* [29] further study the effects of the number of opt-outs displayed in the cookie consent notice. Their results show that the visualization of opt-out choices decreases users' consent but requires more effort than notices with a single purpose (only accept or submit all) button [42]. In binary interfaces (i.e., accept/reject buttons), the users are usually willing to accept the cookies even if the interface lacks a dark pattern technique. These results show the importance of nudging in assisting users in making fully informed decisions when interacting with cookie consent notices. Furthermore, the majority of the current cookie consent notices require excessive effort by users to search for alternatives to the default accept all cookies [33]. It is worth noting that the current landscape of cookie consent notices offers an excellent showcase for studying nudging techniques.

This work differs from the previous ones in evaluating other nudging techniques and their effect on users' decisions. We consider scenarios where website operators use both nudging techniques and dark patterns. We propose the display of: *(i)* opt-out choices in the cookie consent notices (visible and hidden under a button), and *(ii)* a nudging bar that shows the currently enabled cookies using a color-based traffic light-like schema. Color-based nudging has been proved to improve both the strength of passwords [16] and users' privacy in smartphones [13] significantly. Moreover, traffic light color-based nudging can reduce the privacy risks in search engines as shown in [52].

[4] https://darkpatterns.org



(a) Default. (b) Nudging settings. (c) Nudging bar. (d) Nudging settings + bar.

Fig. 1. Cookie consent notices. Figure 1a shows the default notice a participant sees when she starts the survey. Figure 1b shows the first nudging case where the participant does not need to press the "customize" button in order to see the four types of cookie settings. Figure 1c shows the second nudging case where the participant sees a bar the color of which motivates her to change the cookie consent (see Section 3.1). Figure 1d shows a combination of Figures 1b and 1c.

3 USER STUDY

The goal of this study is to explore and describe the effects of nudging, position, and dark patterns in users' answers to cookie consent notices. We define nudging in this work as soft-paternalism towards more privacy-preserving settings in the users' decision-making process, following a similar proposition from Acquisti [1]. Motivated by previous works [29, 36, 46], we focus on further analyzing: *(i)* the effects of nudging in users' cookie consent responses, and *(ii)* how dark patterns affect the effectiveness of the proposed nudged cookie notices. We conduct one counterbalanced experiment, where we evaluate four different cookie consent interfaces, as depicted in Figure 1, that can have one of two possible dark patterns (either Figure 1a or Figure 2), and can be placed in five different positions (see Figure 3). The displayed cookie consent can be ignored (i.e., by not answering) by the participants during the survey, e.g., if the cookie consent is located in the right-bottom corner and does not occlude the survey. We conduct a [1x4x2x5] design that is counterbalanced between-subjects. The independent variables are the *cookie notice type* (default; nudging settings; nudging bar; nudging settings + nudging bar), *dark pattern* (accept default, accept green), and *cookie notice position* (top-left; top-right; bottom-left; bottom-right; center). The primary dependent variable was the *cookie response* (submit default, submit personalized, ignore).

3.1 Independent variables

When designing the survey, we make implementation decisions that aim to isolate the impact of our independent variables and the factors under study and examine possible interaction effects. In more detail, the cookie consent notice consists of a banner on the screen that displays information about the cookies and has two buttons: accept and customize cookies, as presented in Figure 1a. By pressing customize, the banner is extended and lists the following four cookies: essential, site preferences, analytics, and marketing, that are presented in Figure 1b. Essential cookies are always enabled and are not customizable. In general, we covered all possible combinations of the following independent variables uniformly by using a counterbalanced mechanism.

1) Cookie position. Considering that the position of the notice on the screen may affect participants' responses, we replicate the cookie banner positions proposed by the authors of [46]

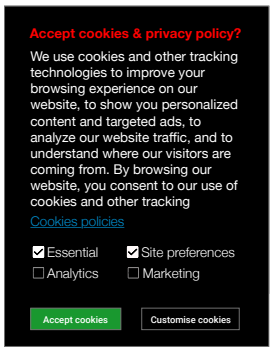


Fig. 2. Cookie notice example with dark pattern where the accept button is in green and the nudging settings visible to the user.

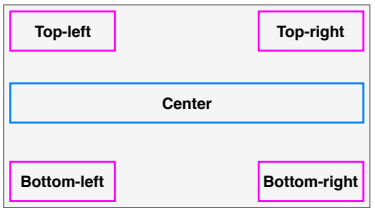


Fig. 3. Positions of the cookie consent notice evaluated.

and examined five different positions: top-left, top-right, center, bottom-left, and bottom-right (see Figure 3). Since the center cookie notice blocks access to the website's information, users have to answer the cookie consent to continue.

2) Dark patterns. We use the commonly-used dark patterns suggested by Utz *et al.* [46] in cookie consent notices by highlighting in green the color of the "Accept cookies" button. Figure 2 depicts an example.

3) Nudging techniques. We use three nudging techniques to influence the users' decision on cookie consent notices:

(1) We present the default settings in the cookie consent, as shown in Figure 1b, instead of hiding them under a menu as visualised in Figure 1a.
(2) We display a simple color-based (red, orange, and green) progress bar, inspired by the traffic-light color scheme used for password creation in the work of Egelman *et al.* [16] and search engine results [52]. The progress bar displays the current privacy threats according to the enabled cookie settings. An example of this technique is presented in Figure 1c.
(3) We employ a combination of the two aforementioned nudging approaches, as visualized in Figure 1d.

Cookie consent design space. There are numerous ways in which interface design choices can be leveraged for nudging or countering dark patterns; we focus our study on two particular design choices. In this paper, we evaluate the participants' responses under the effects of hiding the configuration of cookie settings under the *customize button*. The first one is to opt-out from the default choices, and it has been studied in previous works [29, 46]. It gives us an anchor point to compare the effects of other nudging techniques and dark patterns when combined. The second one is a progress bar which we chose due to its common use in websites in order to strengthen password creation and similar input interfaces. While there have been studies regarding the use of progress bars [16, 52], to the best of our knowledge, this is the first paper to propose it as a nudging tool to influence individuals during cookie consent responses.

We chose our design conditions in order to isolate, as much as possible, the factors under study and examine interaction effects. However, we acknowledge that the current design space can be a limited representation of the design possibilities for cookie consent notices. For example, regarding the color of the cookie consent notice, we chose a dark background color to stand out over the typical white background of most websites. This may have a positive effect on the MTurk workers' interaction with the form, following previous works [46] that use similar colors to stimulate users'

interaction. Other alternatives, such as using a transparent background, may be considered in future work. Likewise, we chose the size of the cookie consent notice so that it does not cover the whole page (e.g., in mobile websites), as this may "force" individuals to respond to the cookie consent with the default values (e.g., "accept") so that they can view the content of the website [46].

Preliminary study for nudging bar. We used the techniques proposed by Ur *et al.* [45] to design our nudging bars. We note that the lack of text in the nudging bar in our survey allows us to display a more compact and straightforward cookie consent notice without limiting the understanding of its functionality. That said, motivated by concerns regarding the participants' level understanding of the nudging bar's functionality, in a preliminary study with 35 MTurk workers (18 male, 17 female, age ranging from 22 to 44), we added these questions at the end of the survey:

- Did you find it easier to understand the number of enabled cookies and privacy risks while using the nudging bar? (Answer: 1-5 Likert scale, 5-Very easy, 1-Very difficult)
- Why was it easy/difficult to understand the number of enabled cookies and privacy risks while using the nudging bar? (Answer: open-ended)

The results indicate that participants ($\chi^2(4) = 5.03,\ p = 0.0011$) did not have a problem understanding how nudging bars work. Participants were able to understand the meaning of the color (green, yellow, orange, red) and the size of the filled bar according to the number of enabled cookie types. Only three participants did not indicate a complete understanding of the purpose of the filled bar and preferred the nudging settings' technique to signal the enabled privacy cookies.

3.2 Evaluation metrics

We evaluate the participants' responses by counting the number of enabled cookie types in the submitted cookie consent notice. According to the authors of [25, 46], users have a very low probability of changing the default cookie settings. Hence a change in the default settings can be interpreted, via inference, as a signal of a conscious choice. Similar to approaches that quantitatively analyze users' behaviour against nudging by using their responses in online social networks [31, 47], we capture participants' cookie notice responses. Hence we can analyze users' behaviour implicitly by considering whether they change the default preferences.

3.3 Participants and Apparatus

Recruitment. We use the Amazon Mechanical Turk (MTurk) crowdsourcing platform to manage our survey using Human Intelligent Tasks (HITs). We recruit 1,100 participants using MTurk. The survey is limited to workers with a 90-100% HIT approval rating, and the number of previous HITs approved greater than 50. We analyze and proofread the answers of the participants before rewarding them. Before posting the survey on MTurk, we ran a pilot study with 50 participants recruited at our university to test and improve our survey features, such as questions and answer options. Each participant received a remuneration of 0.32 USD for completing the survey. Survey participation time ranged between 1.7 to 7 minutes (median: 3.3).

The distribution of gender, age, and education are uniformly spread. Out of 1100 participants, 568 are female, 511 are male, and the remaining are transgender, gender-variant, or preferred not to answer the question. The majority of the participants are below 35 years old (53%), while only 7.6% of them are 55 or above. 40% of participants have a bachelor's degree. 60% of the participants are from North America. 87% of them use ad-blockers, 67% participated using MS Windows, and 75% Google Chrome. Participants show high levels of privacy concerns regarding collection (66% are concerned or very concerned), awareness (67% are concerned or very concerned), and control (75% are concerned or very concerned). It is worth noting that these findings align with the study of Kang *et al.* [23], where authors mention that MTurk workers are more privacy-aware

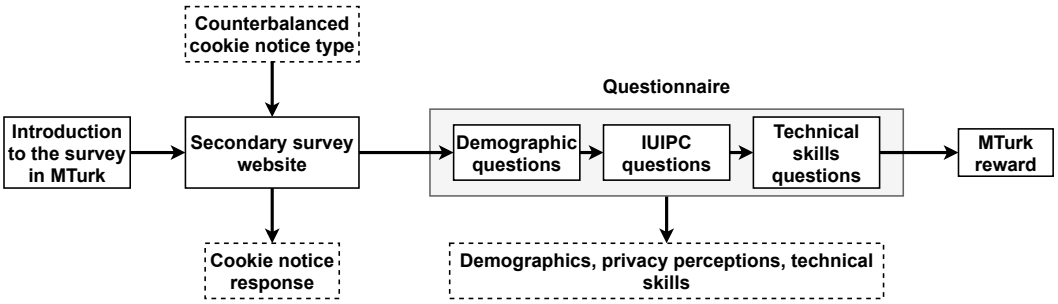


Fig. 4. Study procedure with the generated cookie notices and the responses in dashed boxes.

than the general population. Appendix A describes, in detail, the participants according to their demographics, technical skills, and privacy concern level.

Filtering. Before processing the responses, we filter the ones with the same 'userID' (which is a uniquely generated identification code for each participant after they enter the homepage of the survey) or inappropriately complete surveys (e.g., duration was prohibitively short). After filtering, the remaining participants are 1,100 and we assigned them IDs in the form of P_x with $1 \leq x \leq 1100$.

Apparatus. We deploy our survey in the *heroku* platform.[5] We design and create our survey using SurveyJS.[6] All the collected data is stored in an encrypted MongoDB database in our university.

3.4 Ethics

We informed participants that data would be de-identified, and all recorded data will be password-protected and deleted by the end of the study. Participants provided informed consent to participate in this study. Participants were asked for consent, and it was carried out following the General Data Protection Regulation (GDPR), reviewed, and approved by university IRB regulations.

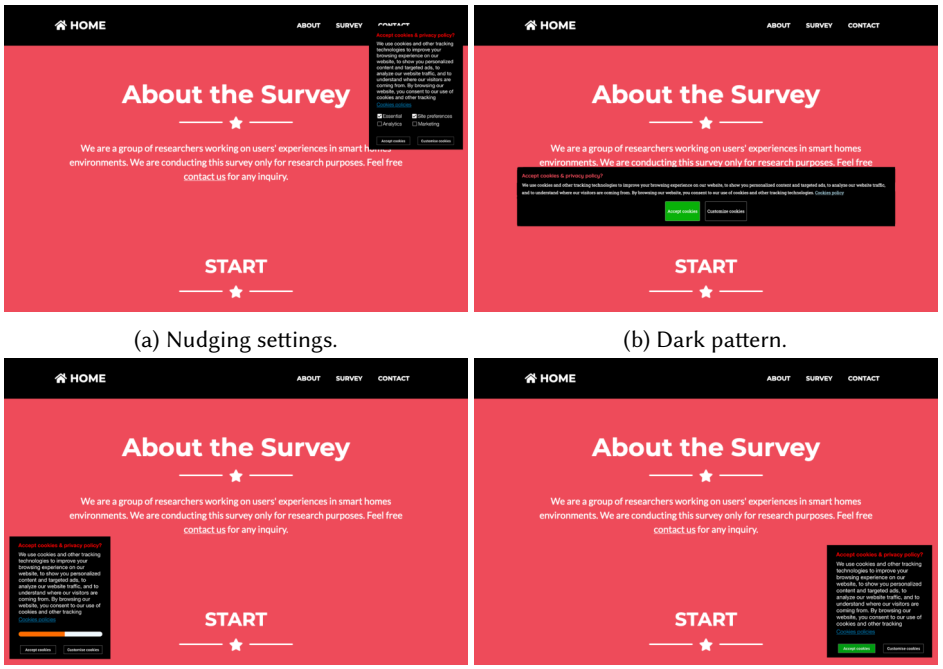
3.5 Ecological validity

We expose participants to secondary survey-related questions that are unrelated to the cookie consent notices. In this secondary survey, we analyze participants' comfort levels in different smart home scenarios. We choose this type of survey as we believe it is an exciting and timely topic that can engage participants [26, 50]. The cookie consent notice is displayed at the beginning of the survey. Questions regarding participants' demographics and privacy concerns are asked at the end. We note that the survey questions presented to the users are not directly related to privacy but their user experience with smart homes. Despite the possible priming effects of the aforementioned smart home questions, our findings regarding the participants' privacy concerns show similar characteristics as previous works [8, 38]. We discuss this in more detail in Section 3.7. Finally, participants are not debriefed regarding our analysis of their cookie-consent responses in order to reduce any possible effect on other subsequent participants' responses [15]. In that sense, we follow the approach of [46], also considering that all the collected data is anonymized [3].

3.6 Procedure

After accepting the MTurk task, each worker is redirected to the survey web page that is specifically designed and developed in order to allow us to collect additional information. The duration of the survey study is approximately 4 minutes. Below we present in detail each step of the designed survey, as shown in Figure 4.

[5] www.heroku.com [6] https://surveyjs.io



(a) Nudging settings.

(b) Dark pattern.

(c) Nudging bar.

(d) Dark pattern.

Fig. 5. Screenshots of different cookie consent notices.

Initial page. Participants are redirected from the MTurk HIT to the homepage of our survey. This page shows a brief description of the goals of the survey study and the people involved. There is also a button that participants should press to start the survey.

Consent and overview page. The second page of the survey contains a consent form that MTurk workers are required to agree with in order to participate in the survey.

Cookie consent notice. After giving consent to participate in the survey, we show workers a cookie consent notice on the first page of the survey, see Figure 5 for a set of examples, similar to Cookiebot.[7] The cookie consent notice follows the general data protection regulation (GDPR; Regulation (EU) 2016/679), where individuals should make informed decisions to give consent to the collection and processing of their data. We collect all cookie consent responses of participants anonymously to provide better insights into the participants' behaviour with the displayed notice.

Secondary survey. On this page, we ask participants to respond to several questions regarding the experience with smart home devices. We design the smart home survey following previous works [5, 28, 34] that use so-called *vignettes* to ask participants about their comfort levels when describing a particular scenario. The vignettes consist of several different scenarios pertaining to the current configuration of a smart device (ON/OFF) in a particular location of a house. The collected data from this part of the survey have not been used in the analysis of this paper, as we solely focus on participants' behaviour when interacting with the cookie consent notices. The analysis of the data collected by the smart home survey will be reported in separate future work that will only focus on that part.

[7] www.cookiebot.com

Dark pattern	Nudging settings	Nudging bar	MTurk	Pilot study
✓	-	-	4.19%	3.12%
✓	✓	-	6.14%	5.13%
✓	-	✓	14.5%	15.67%
✓	✓	✓	16.7%	18.22%
-	-	-	3.02%	4.13%
-	✓	-	4.84%	5.12%
-	-	✓	14.5%	13.11%
-	✓	✓	9.92%	10.04%

Table 2. Participants that changed the default cookie settings, where (✓) illustrates that the nudging/dark pattern technique is active, and (-) that is not displayed.

Demographics and technical skills page. At this stage of the survey, we ask a series of demographic questions such as age, gender, country of residence, followed by multiple-choice answers, and an open-ended option. Participants are asked about their self-reported technical skills levels (1: very weak, 5: very strong) with technology, computer security, and smart home scenarios [51]. A complete list of the survey questions is provided in Appendix A.

Privacy concerns page. The final stage of the survey includes the Internet users' information privacy concerns (IUIPC) survey [30] to understand participants' level of privacy concerns (1: very unconcerned, 5: very concerned). The IUIPC focuses on concerns regarding collection, awareness, and control of personal information. We use the questions in Naeini *et al.* [34] as a reference, which are also provided in Appendix A. Finally, we ask participants if they have seen a cookie consent notice while browsing other websites and are familiar with its function.

3.7 Limitations

Considering the setup of our study, we identify the three following limitations:

1) Crowdsourcing. As highlighted by Kang *et al.* [23], MTurk workers are usually more privacy-aware than the general population [23, 49], while the diversity of their population is more limited [9]. However, according to Redmiles *et al.* [39], MTurk workers provide a more general population sample than other telephone or mailbox methods to survey individuals. The use of crowdsourcing platforms can also raise privacy-related concerns related to the collection and processing of workers' information that can modify the behaviour of MTurk workers [49]. In order to examine how differently traditional participants respond in comparison to MTurk workers, we conducted an initial pilot study with 50 participants at our university (without using MTurk) who showed similar behaviour in their cookie notice responses.

Table 2 depicts the percentage of participants that changed the default cookie settings according to the dependent variables (nudging, dark patterns) used in the cookie consent notice. We can observe that the participants from the MTurk survey and the aforementioned pilot study (non-MTurk workers) have similar behaviour for each cookie consent notice.

2) IUIPC. We acknowledge that placing the IUIPC at the end of the survey can have a priming effect on the related responses [41], given the users' prior interaction with the survey such as demographics and smart home survey. We note that we follow standard practices from previous works about the positioning of IUIPC questions, and our results show similar findings [5, 7, 8, 34, 38], regarding our participants' responses. We also stress that our main study's results regarding cookie consent responses are generally not primed in that sense, as cookie notices are displayed at the

beginning of the survey. More than 99.4% of the participants respond to the cookie consent notice within 34 seconds from the beginning of the survey.

3) Ad-blockers. It is worth noting that 87% of the participants in our study had enabled an ad-blocker that was detected by a script we embedded in the website hosting the survey. Although MTurk workers are considered more privacy-aware in comparison with the general population (47% of users globally[8]), the use of ad-blockers may be related to the intrusive behaviour of online ads [37, 44].

4) GDPR. The exposed population in this study has a different understanding of data protection regulations since not all participants live under the GDPR policy. Differences in privacy regulations can affect the mental models and how participants react to cookie consent notices. We provide an analysis where we compare the participants' behaviour between workers with prior experience with the GDPR cookie consent and those who have not.

4 ANALYSIS OF USER RESPONSES

We analyze the effects of different interface designs (e.g., position, nudging, and dark pattern) on consent responses using the non-parametric Kruskal-Wallis statistical test [27]. To evaluate the importance of the different cookie notice interface designs, we construct a generalized linear mixed model (GLMM) regression with fixed effects, similar to the work of Nouwens *et al.* [36]). We include the position, enabled cookies by default, nudging configuration, and dark patterns (e.g., 0 or 1) as independent variables. The modification of any of the enabled-by-default settings before accepting the cookie (i.e., cookieChanged: 0 or 1) is our dependent model variable. We performed model selection to find the best factors using a backward elimination approach. At each step of the model selection, we eliminate the factors with the largest p-value until we reach the global minimum Bayesian information criterion (BIC) [22]. The model with the lowest BIC best explains the dependent variable. We use a threshold of 0.05 to determine if a factor is significant. These factors help us understand the importance of nudging and dark patterns in users' responses.

4.1 Descriptive analysis

Table 3 shows cookie-related demographics. Most of the participants (86%, n=946) complete the survey and reply to the cookie consent using their desktop/laptop device. One interesting aspect is the widespread use of ad-blockers. As we described in the limitation sections, MTurk workers are characterized as being more privacy concerned than average users, which can explain the high number of participants with ad-blocker enabled. The majority of the participants (86%, n=946) have previous knowledge of cookie consents (we ask participants to provide an explanation about cookies, following [29]). Most participants use Chrome (75%, n=749) to open the survey website, followed by Firefox users (10%, n=99) and Safari users (6%, n=75). As we can observe, most participants (90%, n=990) did not change the default cookie settings despite the nudging techniques. However, our sample of MTurk workers challenges more the modification of default cookies since MTurk workers are financially incentivized to complete the task as soon as possible [24]. Only 28 of the MTurk workers did not interact with the cookie consent notice during the study.

Main factors of cookie interactions. Table 4 depicts the regression model that examines the effect of different predictors for the cookie consent model. The model with nudging, dark patterns, and without interaction has the lowest BIC score. Following similar results than Utz *et al.* [46], the cookie notice position does not have any significant effect on users' cookie consent responses.

[8] www.globalwebindex.com/reports/global-ad-blocking-behaviour

Feature	Category	%	Feature	Category	%
Ad-blocker	enabled	87%	Device	desktop	86%
	disabled	13%		smartphone	12%
Cookie	default	90%		tablet	2%
settings	changed by user	10%	OS	Android	12%
Cookie	bottom right	19%		macOS	14%
position	bottom left	21%		iOS	4%
	center	20%		Windows	67%
	top right	20%		Others	3%
	top left	20%	Browser	Google Chrome	75%
Nudging	Progress bar	23%		Firefox	10%
	Show default cookies	25%		Safari	6%
	Both nudges	23%		Microsoft Edge	5%
Dark pattern	Accept button highlighted	49%		Others	4%
Cookie	Yes	86.2	Display	<500px	13.2
knowledge	No	13.8	width	500px - 1000px	2.45
				>1000px	84.3

Table 3. Cookie demographics for 1100 participants.

Factor	Estimate	Std. Error	Z-value	p-value	BIC
darkPattern	0.38	0.2	1.3	0.018	649
nudgingType	0.288	0.09	3.083	0.002	650

Table 4. GLMM regression output for the two-classes model. We order the factors by their BIC contribution. The factor with the lowest BIC contributes the most to explaining the effects on the use of keywords for the cookie consent.

4.2 Main Findings

Nudging type and cookie interaction. Figure 6 shows the percentage of users that interacted with the cookie consent notice and changed the default settings for different configurations of dark patterns and nudging techniques. One observation is that the nudging bar is the most effective mechanism in influencing the participants to change the default settings, even when used together with dark patterns in the cookie consent notice. For example, when participants are shown a notice with the nudging bar and dark pattern, 14.5% (CI $[8.0, 21.0]$) of them deviate from the default settings, whereas the corresponding percentage when shown a notice only the dark pattern is 4.19% (CI $[1.0, 9.0]$). In general, nudging techniques appear to increase the percentage of users that deviate from the default settings. On the contrary, dark patterns do not seem to significantly affect steering users towards accepting the default cookie settings. When using dark patterns and nudging mechanisms, a higher percentage of users (16.7%) opt to change the default settings. That said, similar to previous works [29, 46], the overall level of user engagement with cookie consent notices, beyond accepting the default configuration, is low, which makes it hard to draw definitive conclusions. A pairwise Kruskal-Wallis analysis shows that there is a significant effect ($\chi^2(2) = 6.68,\ p < 0.05$) of nudging with the cookie consent. The nudging bar approach shows better results in the user interaction with the cookie consent. In the cookie notices where the

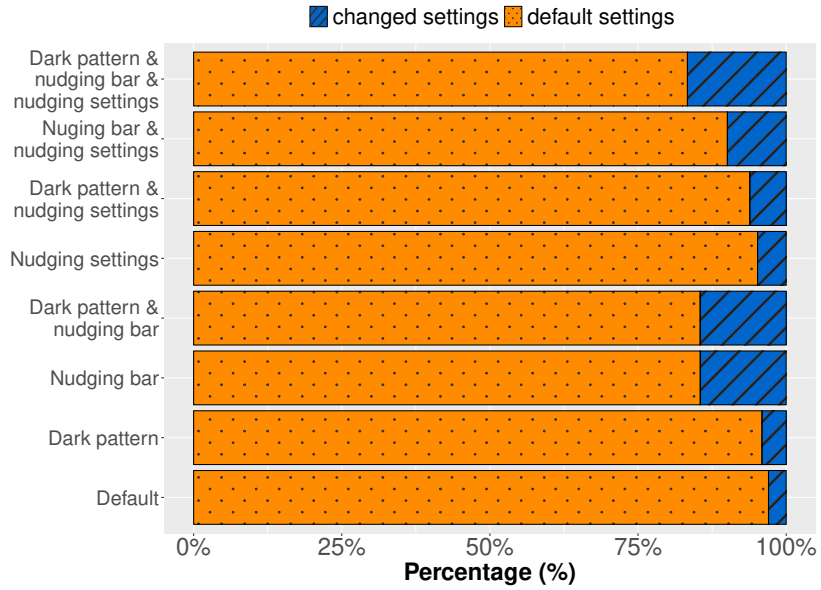


Fig. 6. Interaction rates with the cookie consent, where *changed settings* means that the participants changed the default displayed cookie settings and *default settings* that they did not change them.

nudging bar is displayed (either alone or in combination with the nudging choices), participants modify the default values of the enabled cookies with higher probability (71%, n=77).

Ad-blocker and cookie interaction. Our results show a significant impact of ad-blocker usage on users' behaviour. A pairwise Kruskal-Wallis analysis shows that there is a significant effect ($\chi^2(1) = 7.86,\ p < .001$) of the ad-blocker usage on the cookie consent responses. Participants that do not use an ad-blocker are very likely (2%, n=19) to accept the default cookie settings.

Privacy attitudes and cookie interaction. We found that nudging only works on participants that tend to assume a more active role in controlling their privacy. A pairwise Kruskal-Wallis analysis shows the significant effect ($\chi^2(2) = 3.86,\ p < .05$) of privacy concerns on consent responses. Our results, contrary to previous show that users with more severe privacy concerns are more willing (10.5%, n=217) to change the default displayed cookies.

4.3 Time and cookie interactions

As shown in Figure 7, on average participants take 12.18 seconds (median: 7 seconds) to respond to the cookie consent notice. When the nudging settings mechanism is displayed (dashed blue line), most participants (99.6%) out of those that do not modify the current default settings respond to the cookie consent notice within 21 seconds, whereas most participants (99.3%) out of those that do modify the current default settings respond within 31 seconds. Focusing on the cases where participants modify the default cookie settings (figure on the right side), we observe that more than 99.8% modify the cookie consent with the progress bar nudging within 25 seconds, while 99.3% respond within 31 seconds when the nudging settings is used. On many occasions, the location of the cookie consent does not block the information (e.g., top-right, bottom-right), primarily when participants use wide screens. As a result, some participants did not reply to cookie consent (4%, n=44). A pairwise Kruskal-Wallis analysis shows that there is a significant effect

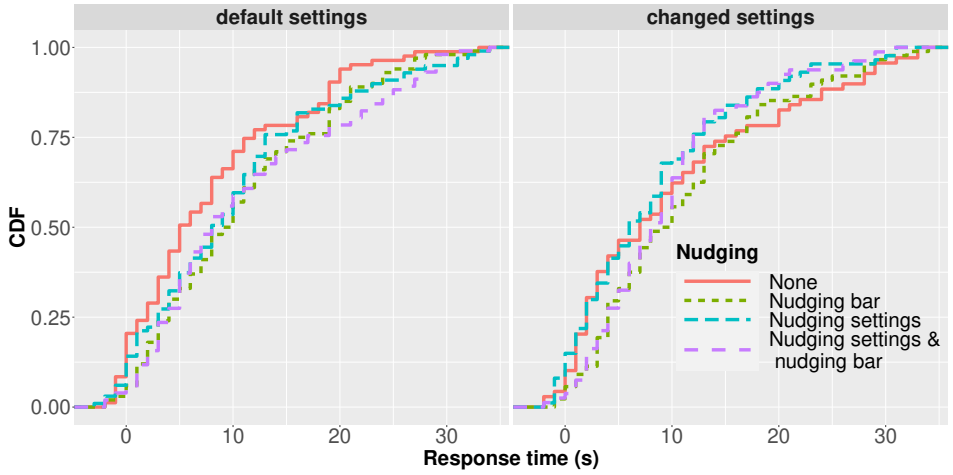


Fig. 7. Cumulative distribution function (CDF) of time to respond to the cookie notice according to different nudging configurations. *Default settings* (left) means that participants did not alter the default displayed cookie settings, whereas *changed settings* (right) means that participants altered the default settings.

($\chi^2(4) = 8.32,\ p = 0.0039$) of the nudging condition used in the time the participants spend to respond to the cookie consent. When the cookie consent contains nudging settings (opt-out visible), the participants (43%, n= 66) take an average of 19 seconds to change the default cookie settings and accept the cookie consent. On the contrary, in the cookie consent notices nudged only by the bar (no opt-out visible), the participants (60%, n=45) take an average of 16.5 seconds. In the latter, nudging participants still have to click the button "customize cookies" to display and be able to modify them.

4.4 Device type and cookie interactions

When the cookie consent notices pop up on their smartphone displays, the behaviour of participants is significantly different from when they interact with desktop/laptop versions. The cookie consent notice interrupts participants' interactions with the website due to the reduced size of smartphone displays. Our results show that participants using a smartphone have shorter reactions with the cookie consent notice (12 sec.) than participants of desktop/laptop (13.2 sec.) and that these interactions are mainly to accept the default cookies.

4.5 OS, browser and cookie interactions

A pairwise Kruskal-Wallis analysis shows that there is no significant effect of the OS used on the interaction behaviour with the cookie consent notice ($\chi^2(4) = 19.45,\ p = 0.59$). Similarly, the browser used to complete the survey has a small impact on whether someone interacted with the cookie consent notice. A pairwise Kruskal-Wallis analysis shows that there is no significant effect ($\chi^2(4) = 4.88,\ p = 0.99$) of the browser used to complete the survey on the cookie consent responses. Firefox users (10%, n=99) and Opera users (9%, n=99) seem more active to change the default settings in comparison to users of other browsers (e.g., only 7% (n=53) of the Chrome users change the default behaviour of the cookie notice). Following the news about the privacy issues in

Google Chrome[9] it is interesting to highlight that users that use Chrome have smaller probability (7%, CI [2.0, 11.0]) to change the default privacy settings than Firefox users (11%, CI [6.0, 18.0]).

4.6 Cookie notice position and interactions

The cookie position does not have a significant effect on participants' interaction with the notice. Although there are differences in the change of the displayed defaults of participants when the cookie notices are in the bottom left or right of the screen, a pairwise Kruskal-Wallis analysis show that the effect is not significant ($\chi^2(4) = 1.63,\ p = 0.8$). This result follows similar findings to Utz *et al.* [46], where authors study the effects of cookie position and find no significant effect of position in users' responses.

4.7 Cookie consent settings and interaction

The cookie consent settings (i.e., enabled cookies by default) do not significantly affect participants' interactions with the notice. A pairwise Kruskal-Wallis analysis shows that there is no significant effect ($\chi^2(4) = 3.79,\ p = 0.8754$) of the enabled cookie types in the participants' cookie responses. This shows that, independently of the enabled cookies configuration, the evaluated nudging techniques work and influence participants to change the default behaviour of the cookie consent.

4.8 Dark pattern and cookie interaction

The addition of the dark pattern in the cookie notice (i.e., green highlight accept button) influences users' interaction with the notice. A pairwise Kruskal-Wallis analysis shows that there is a significant effect ($\chi^2(1) = 0.33573,\ p = 0.0056$) of the dark pattern on users' interactions.

4.9 Technical skills and cookie interaction

The self-reported familiarity of computer security ($\chi^2(3) = 1.47,\ p < .001$) shows significant effect on cookie consent responses. Participants with higher self-reported familiarity of computer security have a higher probability (12%) to change the default cookie settings than participants with lower self-reported familiarity.

4.10 GDPR

Even if users are not EU citizens, the regulations of GDPR can request websites to provide cookie consent notices to individuals outside the EU whenever the website they access is hosted inside the EU [18]. Our survey gauges individuals' familiarity with GDPR cookie consent notices by asking participants the question: "*Have you ever interacted with cookie consent notices (e.g., the pop-up menu at the beginning) before this survey?*" 86.3% (n=946) of the participants responded positively to the question. However, it is worth noting that, according to the collected responses, the probability of a participant changing the default settings in a cookie consent is 10% (n=110), and it is independent of whether the participant is familiar with GDPR or not.

5 DISCUSSION

Summary of findings. Our work shows the effects of using nudging in scenarios where "deceiving" interface designs, such as dark patterns, are deployed. We observed that the participants are more likely to modify the default cookie settings when cookie consent notices include the nudging bar. This highlights the potential of nudging for helping users make more informed decisions about their

[9] www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch

privacy and the possibility that nudging may help counterbalance current dark pattern techniques, such as highlighting the "accept" button. In scenarios where only our proposed nudging techniques are shown to participants (nudging settings, progress bar), there is an increment of 14% in the probability of modifying the current default behaviour of cookie consent notices. However, we note that the limited number of participants who do change the cookie consent's default behaviour echoes the difficulties discussed in previous works regarding the engagement of users with cookie consent [29, 46]. Below we attempt to interpret our main findings.

- **Nudging type and cookie interaction.** The use of nudging in the notices, despite the existence of dark patterns, shows an increment in the probability that participants alter the default cookies. The willingness of participants to modify the default cookies increases when the nudging displayed includes one of the interface variants with the nudging bar.

- **Ad-blocker and cookie interaction.** Motivated by the analysis in Utz *et al.* [46] about ad-blockers and users' interactions with the cookie notice, we evaluate the behaviour of participants according to whether they use an ad-blocker or not. Interestingly enough, and in contrast with the findings of Utz *et al.* [46], our results show a significant impact of ad-blocker usage on users' behaviour. Participants that do not use ad-blocker have very low probability of materially interacting with the cookie consent (i.e., modifying the current default cookies).

- **Privacy attitudes and cookie interaction.** We found that nudging is more effective on participants with stronger privacy concerns since we observed a higher probability of them modifying the default cookie settings. Our results, build on top of the findings of previous work [29] where the participants with stronger privacy concerns consent to fewer enabled cookie settings. This result seems to challenge the *privacy-paradox* [35]. Although, we should interpret these results with caution due to the specific domain nature of our study (i.e., cookie consent notices) and the relationship between privacy attitude and cookie consent responses in nudged environments.

Comparison with prior work. Prior works such as Utz et al. [46] and Machuletz et al. [29] analyze users' interactions with cookie consent notices according to dark patterns (highlighting the accept button) and nudging techniques (visualization of cookie settings). In this work, we consider a different design space for both nudging techniques and dark patterns. We study a combination of interfaces analyzed in prior works [29, 46] with the addition of hiding the cookie settings under a button (*customize cookies*). In contrast with previous work, our interface design hides the cookie settings, thus increasing the participants' effort when modifying the default cookie settings. This is likely to reduce the effects of nudging techniques as it requires the participants to engage more in the modification of the default cookie settings [29]. Moreover, we also propose the display of a nudging bar that shows currently enabled cookies using a color-based traffic light-like schema. Our work shows positive results for nudging in the presence of dark patterns and how users can benefit from nudged designs to provide more informed cookie consents.

Future directions. Our study leaves many interesting directions for future work. For example, it would be informative to include a broader design space to create cookie consent notices, such as variable background color and size. The design of different background styles (e.g., transparent) can provide interesting findings regarding the effect this has on users' decisions; to the best of our knowledge, it does not exist a systematic evaluation these factors. Another potential design study could be on additional options for the user to interact with the cookie consent notice (e.g., an accept-only-essential-cookies button). Moreover, commonly used cookie consent designs for mobile environments typically involve notices that can cover the entire screen, blocking the visitor's access

to the website and "demanding" her response in order to continue navigation (usually including dark patterns in the process). This can again drastically affect users' interaction with cookie consent notices in the mobile setting. Finally, future studies can include other nudging techniques that can be used in the context of cookie consent, such as timer nudging [48], or confirmation nudging ("Are you sure you want to proceed?").

Ensuring that users are fully informed during their privacy-related decision-making process is an important topic in the community. Several previous studies have focused on studying how the interface design approaches can influence users [29, 32, 36, 46]. These studies typically focus on either tricking users into giving away additional information (dark patterns) [32, 36] or towards more privacy-sensitive configurations (i.e., nudging) [29, 46]. We hope that the findings from our combined study can provide a better understanding of the effects of each design approach and how future interfaces can counterbalance current and more common dark pattern techniques. In view of our results, nudging techniques, such as the progress bar, can impact users' decisions even in scenarios where dark patterns are still present. We can still find dark patterns and other strategies to circumvent the *GDPR-by-design* in new websites that are built to ensure compliance with the GDPR [40]. Insights from the use and impact of dark patterns and nudging in users' responses can be useful in other scenarios with similar graphical user interfaces (e.g., privacy settings in online services such as social networks [47]).

6 CONCLUSION

In this paper, we evaluate how different nudging techniques can influence users that interact with cookie consent notices to change the default cookie settings. We analyze users' responses when multiple nudging techniques are combined (e.g., nudging settings and nudging bar) and when they coexist with dark patterns. Our results show that nudging techniques can increase by 14% the probability of a user changing the default setting. Differing from previous studies [29, 36] that show the benefits of displaying the purposes of the cookies in the notice, our results show that a progress bar that depicts the number of enabled cookies and changes color based on this number (green when all the cookies are disabled and red when all are enabled) has a stronger influence on users responses. Our results align with previous findings [46] that support that the position of the cookie notice, even when it blocks the information of the website (e.g., center position), does not have a significant effect on the consent responses. Notably, our results show that nudging techniques can persuade even users who are financially incentivized to complete a browser-based task (e.g., MTurk workers) as soon as possible to change the default settings. It is also worth noting that our findings contradict the so-called "privacy paradox" [35], where privacy-aware participants modify the default cookie settings.

Numerous studies focus on employing nudging techniques to inform users about privacy policies and assist them in making more privacy-aware decisions. However, all these nudging techniques are effective only if they are implemented into industry standards [36]. Studying user responses with different designs may be helpful beyond the particular application of cookie consent notices to analyze the visual biases that may be rendered by such designs more generally. We believe our findings can be applied as the groundwork for designing better cookie consent notices in ways that website operators can adopt.

7 ACKNOWLEDGEMENTS

We thank our undergraduate researcher assistant for their help during the coding of the participants' comments. This research has been supported in part by project 16214817 from the Research Grants Council of Hong Kong, and the 5GEAR project (Grant No. 318927) and the FIT project (Grant No. 325570) funded by the Academy of Finland.

REFERENCES

[1] Alessandro Acquisti. 2009. Nudging privacy: The behavioral economics of personal information. *IEEE security & privacy* 7, 6 (2009), 82–85.

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 44.

[3] Eytan Adar, Desney S Tan, and Jaime Teevan. 2013. Benevolent deception in human computer interaction. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1863–1872.

[4] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. ACM, 787–796.

[5] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 59.

[6] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. 2018. A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces. In *23rd International Conference on Intelligent User Interfaces*. ACM, 165–176.

[7] Natã Miccael Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. " What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *PoPETs* 2019, 4 (2019), 211–231.

[8] Natã M Barbosa, Zhuohao Zhang, and Yang Wang. 2020. Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)*. 417–435.

[9] Christoph Bartneck, Andreas Duenser, Elena Moltchanova, and Karolina Zawieska. 2015. Comparing the similarity of responses received from studies in Amazon's Mechanical Turk to studies conducted online and with direct recruitment. *PloS one* 10, 4 (2015).

[10] Rainer Böhme and Stefan Köpsell. 2010. Trained to accept? A field experiment on consent dialogs. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 2403–2406.

[11] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 2019. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–15.

[12] Fred H Cate. 2010. The limits of notice and choice. *IEEE Security & Privacy* 8, 2 (2010), 59–62.

[13] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. 2013. Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction*. Springer, 74–91.

[14] Henrik Cronqvist and Richard H Thaler. 2004. Design choices in privatized social-security systems: Learning from the Swedish experience. *American Economic Review* 94, 2 (2004), 424–428.

[15] Greg d'Eon, Joslin Goh, Kate Larson, and Edith Law. 2019. Paying Crowd Workers for Collaborative Work. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[16] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my password go up to eleven? The impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2379–2388.

[17] Steven Englehardt and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 1388–1401.

[18] Michelle Goddard. 2017. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research* 59, 6 (2017), 703–705.

[19] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–14.

[20] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. " It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[21] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. 471–478.

[22] Joseph B Kadane and Nicole A Lazar. 2004. Methods and criteria for model selection. *Journal of the American statistical Association* 99, 465 (2004), 279–290.

[23] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of mechanical turk workers and the us public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 37–49.

[24] Steven Komarov, Katharina Reinecke, and Krzysztof Z Gajos. 2013. Crowdsourcing performance evaluations of user interfaces. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 207–216.

[25] David M Kristol. 2001. HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology (TOIT)* 1, 2 (2001), 151–198.
[26] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J Wisniewski. 2021. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–27.
[27] William H Kruskal and W Allen Wallis. 1952. Use of ranks in one-criterion variance analysis. *Journal of the American statistical Association* 47, 260 (1952), 583–621.
[28] Hosub Lee and Alfred Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. IEEE, 407–412.
[29] 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.
[30] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.
[31] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. 2020. Exploring Nudge Designs to Help Adolescent SNS Users Avoid Privacy and Safety Threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–11.
[32] 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.
[33] Lynette I Millett, Batya Friedman, and Edward Felten. 2001. Cookies and web browser design: Toward realizing informed consent online. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 46–52.
[34] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 399–412.
[35] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs* 41, 1 (2007), 100–126.
[36] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns Post-GDPR: Scraping Consent Interface Designs and Demonstrating their Influence. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2020)*. ACM.
[37] Enric Pujol, Oliver Hohlfeld, and Anja Feldmann. 2015. Annoyed users: Ads and ad-block usage in the wild. In *Proceedings of the 2015 Internet Measurement Conference*. 93–106.
[38] Frederic Raber and Antonio Krüger. 2018. Deriving privacy settings for location sharing: Are context factors always the best choice?. In *2018 IEEE Symposium on Privacy-Aware Computing (PAC)*. IEEE, 86–94.
[39] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.
[40] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. Circumvention by design-dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. 1–12.
[41] Jennifer R Steele and Nalini Ambady. 2006. "Math is Hard!" The effect of gender priming on women's attitudes. *Journal of Experimental Social Psychology* 42, 4 (2006), 428–436.
[42] Karen Tang, Jason Hong, and Dan Siewiorek. 2012. The implications of offering more disclosure choices for social location sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 391–394.
[43] Richard H Thaler and Cass R Sunstein. 2009. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.
[44] Panagiotis Tigas, Samuel T King, Benjamin Livshits, et al. 2019. Percival: Making In-Browser Perceptual Ad Blocking Practical With Deep Learning. *arXiv preprint arXiv:1905.07444* (2019).
[45] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, et al. 2012. How does your password measure up? the effect of strength meters on password creation. In *Presented as part of the 21st {USENIX} Security Symposium*. 65–80.
[46] 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*. 973–990.
[47] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 2367–2376.
[48] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy nudges for social media: an exploratory Facebook study. In *Proceedings of the 22nd international conference on*

world wide web. 763–770.

[49] Huichuan Xia, Yang Wang, Yun Huang, and Anuj Shah. 2017. " Our Privacy Needs to be Protected at All Costs" Crowd Workers' Privacy Experiences on Amazon Mechanical Turk. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–22.

[50] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[51] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 65–80.

[52] Steven Zimmerman, Alistair Thorpe, Chris Fox, and Udo Kruschwitz. 2019. Privacy Nudging in Search: Investigating Potential Impacts. In *Proceedings of the 2019 Conference on Human Information Interaction and Retrieval*. 283–287.

A APPENDIX: SURVEY QUESTIONS

A.1 Electronic consent

Your participation in this research study is voluntary. You may choose not to participate. No data will be collected from participants who choose to 'opt-out' during the research process; their data will be immediately destroyed. We will do our best to keep your information confidential. All data is stored in a password-protected electronic format, and any personal information will be securely anonymized during the experiment. We additionally collect browser version and operating system information for demographic purposes. To help protect your confidentiality, the survey does not contain information that can personally identify you. The results of this study will be used for research purposes only. The results of this study can improve the current user interfaces and interactions with online services, with better privacy threat descriptions and more useful information to users.

Please select your choice below:

- Agree
- Disagree (end survey)

A.2 Demographic questions

(1) What is your gender?

- Prefer not to answer
- Male
- Female
- Gender
- Variant/Non-Conforming
- Transgender
- Not listed (Answer: open-ended)

(2) What is your age?

- 18 to 24
- 25 to 34
- 35 to 44
- 45 to 54
- 55 to 64
- 65 to 74
- 75 or older
- Prefer not to answer

(3) Education

- Less than high school degree
- High school degree or equivalent
- Some college but no degree
- Associate degree
- Bachelor degree
- Graduate degree
- Postgraduate degree
- Other (Answer: open-ended)

(4) What is your profession? (Answer: open-ended)
(5) Country of residence (Answer: open-ended)

A.3 Demographics

Table 5 depicts the demographics of our participants and includes their privacy concerns (1 to 5 Likert-scale) and self-reported familiarity.

Demographic	Category	%	Category	%
Basic Demographics				
Gender	male	46%	female	52%
	prefer not to answer	0.9%	gender variant	0.4%
	transgender	0.5%		
Age	18 to 24	13.5%	25 to 34	40.3%
	35 to 44	24.6%	45 to 54	13.1%
	55 to 64	5%	65 to 74	2.3%
	75 or older	0.3%	Prefer not to answer	0.4%
Education	Associate degree	9%	Bachelor degree	40%
	Graduate degree	13%	High school degree or equivalent (e.g., GED)	10%
	I am in the process of getting a professional degree	0.5%	Less than high school degree	0.5%
	Postgraduate degree	11%	Some college but no degree	16%
Regions	South Asia	25%	South America	2%
	North America	55%	Europe	17%
	Others	1%		
Internet Users' Information Privacy Concerns (IUIPC)				
IUIPC Factors	Collection 1, 2, 3	34% ($\bar{M}$: 3.9 CI : [3.8, 3.9])	4, 5	66%
	Awareness 1, 2, 3	33% ($\bar{M}$: 3.7 CI : [3.7, 3.8])	4, 5	67%
	Control 1, 2, 3	25% ($\bar{M}$: 3.5 CI : [3.4, 3.5])	4, 5	75%
Familiarity				
Technology	1, 2, 3	43% ($\bar{M}$: 3.71 CI : [3.61, 3.81])	4, 5	57%
Smart homes	1, 2, 3	23% ($\bar{M}$: 4.12 CI : [4.02, 4.22])	4, 5	77%
Computer security	1, 2, 3	48% ($\bar{M}$: 2.34 CI : [2.23, 2.45])	4, 5	52%

Table 5. Demographics for 1100 participants.

A.4 Questions on technical skills

Participants reported their technical skills with three questions on a Likert-scale from 5-'Very weak' to 1-'Very strong'.
(1) How would you rate your knowledge of technology in general?
(2) How would you rate your knowledge of smart home technology?
(3) How would you rate your knowledge of computer security?

A.5 Previous cookie consent experience

(1) Have you ever interact with cookie consent notices (e.g., pop-up menu at the beginning) before this survey?

A.6 IUIPC questions

Participants answered the following questions [34] on a Likert-scale from 5-'Very concerned' to 1-'Very unconcerned'.
(1) When online companies ask me for personal information, I sometimes think twice before providing it.
(2) It bothers me to give personal information to so many online companies.
(3) Companies seeking information online should disclose the way the data are collected, processed, and used.
(4) It usually bothers me when online companies ask me for personal information.
(5) Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
(6) Consumer control of personal information lies at the heart of consumer privacy.

Received January 2021 ; revised April 2021 ; accepted May 2021