DOI: 10.2478/9788366675896-004 • Technikpsychologie • 41-54

Proceedings of the International Symposium on Technikpsychologie

Defeating Dark Patterns: The impact of supporting information on dark patterns and cookie privacy decisions

Jennifer Klütsch[1,†], Christian Böffel[1,†], Sophia von Salm-Hoogstraeten[1,2,†], Sabine J. Schlittmeier[1,†]

[1]RWTH Aachen Professorship for Work and Engineering Psychology Jägerstr. 17-19 52056 Aachen, Germany
[2]Saint Gobain Research Germany Glasstraße 152134 Herzogenrath, Germany

Abstract

In our daily usage of websites, we face a multitude of privacy decisions. However, as users often lack the knowledge, motivation or time for these decisions, they are vulnerable to privacy-unfriendly designs, so-called dark patterns. To promote deliberate cookie decisions even in presence of dark patterns, the present study investigates, within an experimental online-study (N = 207), the effectiveness of a knowledge intervention. During cookie decisions, either a knowledge intervention in the form of decision-supporting information ("cookie assistance") or no such information (instead an add) were presented. The intervention effects on deliberation, reaction time and cookie activation were investigated, in the presence and absence of dark patterns. Results indicate that supporting information neither stimulated more deliberate and slower reactions nor encouraged participants to make privacy-friendlier decisions in the presence of dark patterns. Instead, evidence for highly conditioned decision-making was found. Practical implications for future privacy-interventions and legal regulations are discussed.

Keywords

privacy • cookies • dark patterns • information

1. Introduction

Users face a multitude of privacy decisions in their daily life. They decide on privacy policies when creating user accounts, on access authorizations when using apps or on web cookies when visiting websites. However, even though users are expected to make deliberate privacy decisions, with the General Data Protection Regulation (short: GDPR) specifying that their consent must be "freely given, specific, informed and unambiguous" (GDPR, 2016, p. 6), researchers argue that most users still tend to make uninformed decisions on privacy policies or web cookies (e.g., Graßl et al., 2021; Gray et al., 2018; Machuletz & Böhme, 2020; Utz et al., 2019). This could be due to the fact, that users face difficulties in balancing perceived risks (e.g., release of personal data) and benefits (e.g., social affiliation, discounts) of privacy decisions equally, as assumed by the privacy calculus theory by Culnan and Armstrong (1999, see, Barth & de Jong, 2017; Kokolakis, 2017, for a review). One reason could be that the storage and processing of personal data are often not users' primary task (Acquisti et al., 2017) or that users lack motivation, knowledge, ability, or time for deliberated risk assessments (Bösch et al., 2016). Thus, users could rely on automatic, fast, and effortless processing rather than slow, effortful, and deliberate processing (see, Barth & de Jong, 2017, for a review). They might base their decisions on incomplete information, information asymmetries, heuristics, biases and other context-dependent factors (see, Acquisti et al., 2017; Kokolakis, 2017, for a review). For instance, during large-scaled analysis of users' behavior on Facebook, Gross and Acquisti (2005) found first evidence that privacy decisions are influenced by default settings. Even if participants had the option to change their default settings and limit their personal data release, most kept the default option and provided large amounts of personal data to Facebook (Gross & Acquisti, 2005). Moreover, Acquisti et al. (2013) demonstrated that users' privacy decisions are biased through loss aversion or order effects as participants appreciated the receipt of personal data (potential loss) more than the protection of public data (potential

[†]Corresponding author: Jennifer Klütsch; Christian Böffel; Sophia von Salm-Hoogstraeten; Sabine J. Schlittmeier
E-mail: kluetsch@psych.rwth-aachen.de; christian.boeffel@psych. rwth-aachen.de; sophia.von.salm@ outlook.de; sabine.schlittmeier@ psych.rwth-aachen.de

Open Access. © 2023 Klütsch et al., published by Sciendo
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

gain) and this behavior was influenced by the order of the data offer. To improve informed and deliberate privacy decisions by the user, the present study examines the effectiveness of supporting information during the cookie decision itself and the role of so-called *dark patterns*. Such deliberately chosen design choices represent major security threats and could tempt users to increased disclosure of personal data.

Dark patterns and web cookies

By hiding information to discourage certain options or by redirected expected functionalities (Gray et al., 2018), *dark patterns* manipulate users' accessible number of choices or their accessible information (Mathur et al., 2021) to guide them to the privacy-unfriendly option. In other words, they "(trick) users into performing unintended and unwanted actions, based on a misleading interface design" (Bösch et al., 2016, p. 239). *Dark patterns* are one type of nudge (Acquisti et al., 2017) in which a nudge describe "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives" (Thaler & Sunstein, 2008, p. 6). Consequently, these *dark patterns* counteract legal efforts by the European General Data Protection Regulation (GDPR) as they support unintended rather than informed privacy decisions (e.g., Graßl et al., 2021; Machuletz & Böhme, 2020; Nouwens et al., 2020; Utz et al., 2019).

Unfortunately, *dark patterns* are common practice on various online services, e.g., within web cookie banners. For instance, during large-scaled analysis of 11,000 e-commerce websites, more than 11% implemented at least one dark pattern (Mathur et al., 2019). Further, even if websites should, according to the GDPR, include cookie banners where (1) consent needs to be explicit, (2) consent and withdrawal are equally difficult, as well as (3) no non-necessary purposes or vendors are preselected (Nouwens et al., 2020), Nouwens et al. (2020) found evidence that only about one tenth of examined websites adhered to all three requirements. As web cookies represent the most used tracking method and are able to track online-behavior for advertisement or analytics (Sanchez-Rola et al., 2019), they represent a major security gap in users' lives that is particularly devious when combined with dark patterns. For example, hiding the reject-button or showing bulk options increased users' cookie acceptance (Nouwens et al., 2020). Additionally, a large-scaled study by Utz et al. (2019) demonstrated that cookie banner positions and certain cookie types increased interaction rate or cookie activation. For instance, the researchers observed increased cookie activation when dark patterns such as pre-selected checkboxes were presented (Utz et al., 2019).

The multitude of privacy risks associated with web cookies and implemented dark patterns underscore the importance to investigate why dark patterns influence privacy behavior and to derive interventions that counteract their impact. The Dual Process Model by Kahneman (2003) is a framework that can be used to explain how dark patterns impact decision making. It distinguishes two systems of cognitive processes: (1) *System 1*, referring to automatic, fast, and effortless thinking and reasoning processes, and (2) *System 2*, referring to slower, effortful, and deliberated processes (Kahneman, 2003). As users often lack the motivation, ability, knowledge, or time for privacy decisions, most privacy decisions rely on automatic, fast, and effortless *System 1* (Bösch et al., 2016). For instance, when users visit a website, they are interested in using a service whereas the associated cookie decision is rather incidental. Users often make such a decision fast and without much effort, because their motivation and time to engage with the cookie banner are limited. Additionally, information provided by cookie banners is often needlessly complex or detailed, users' knowledge about the topic limited and their ability to make a deliberate privacy decision low. However, as users do not deliberate their decision in *System 1* processing, they are influenced by heuristics and biases and tend to focus on the highlighted and simplest option. They are also less aware to notice dark patterns and, thus, cannot counteract them (Bösch et al., 2016). First empirical results on users' awareness of dark patterns emphasize the assumption that users rely on *System 1* processing. Although, users are generally aware of deceptive design choices (Maier & Harr, 2020) and their impact on users' behavior (Bongard-Blanchy et al., 2021), they are unable to detect or unsure about dark patterns that prevail during their privacy decisions and underestimate the harm to themselves (Bongard-Blanchy et al., 2021; Di Geronimo et al., 2020). However, their detection of dark patterns is improved when they are primed or informed (Di Geronimo et al., 2020).

Improving privacy-friendly decisions by interventions

Integrating the theoretical and empirical insights, interventions would have to either guide *System 1* processing into privacy-friendly directions (e.g., Dennis & Minas, 2018; Sunstein & Reisch, 2019) or trigger *System 2* processing by increasing motivation as well as knowledge (e.g., Bösch et al., 2016; Sunstein & Reisch, 2019). Besides, interventions could encourage users' general competencies as suggested by Hertwig and Grüne-Yanoff (2017). Thus, Graßl et al. (2021) highlight the importance of three intervention approaches: (1) *non-educative nudges* to guide users' System 1 processing to the privacy-friendly option, (2) *educative nudges* to induce *System 2* processing (Sunstein & Reisch, 2019) or (3) *long-term boosts* to generally enhance users' competencies (Hertwig & Grüne-Yanoff, 2017).

The first intervention approach—*non-educative nudges*—refers to nudges that guide users' behavior towards one desired

outcome without intending to increase users' ability to choose with privacy-friendly settings (Sunstein & Reisch, 2019). One example for *non-educative nudges* are *bright patterns* that guide users to the privacy-friendly option and quickly and effectively reduce privacy risks (Graßl et al., 2021). For instance, Graßl et al. (2021) reversed default options or obstructions in cookie banners to bright patterns and demonstrated a corresponding increase on users' cookie rejections as an indicator for privacy-friendly behavior—. Nevertheless, like *dark patterns*, non-educative nudges exploit cognitive heuristics and biases (Hertwig & Grüne-Yanoff, 2017). Rather than enhancing users' reflective thinking, interventions such as *bright patterns* trigger unreflective *System 1* processing (Graßl et al., 2021; Hertwig & Grüne-Yanoff, 2017). Yet even *bright patterns* are successful interventions to encourage more privacy-friendly behavior, the negative effects of *dark patterns* are not reduced the next time they appear.

Therefore, the present study focuses on so-called *educative nudges* to counteract the impact of dark patterns. *Educative nudges* such as reminders or warnings are designed to trigger users' *System 2* processing (Graßl et al., 2021; Sunstein & Reisch, 2019). Examples for *educative nudges* could be interruptions that emphasize potential dangers (fear appeal), highlight unintentional data disclosures and its potential counter measurements (warnings), highlight the most important information (attractors) (Distler et al., 2020), or prepare comprehensible information (disclosure requirements) (Sunstein, 2016). First empirical results showed their effectiveness.; for example, Harbach et al. (2014) visualized Android app permissions with personalized examples (e.g., users' shared photos or locations) as well as highlighted accompanied dangers and found evidence that these modified permissions caused fear and guided users to the privacy-friendly decision. Nevertheless, it should be noted that these *educative nudges* (e.g., fear appeals) raise ethical questions as it is unclear whether a deliberated or a fear-led decision is encouraged (Distler et al., 2020). Rather than inducing fear, *educative nudges* can provide users with knowledge to make a deliberated cookie decision (Sunstein, 2016; Sunstein & Reisch, 2019), for instance, by providing feedback on consequences of certain cookie decisions (Graßl et al., 2021). However, it remains unclear how these types of educative nudges should be implemented as well as how and which kind of information should be presented to improve knowledge and motivation (cf. Graßl et al., 2021).

The present study

Overall, the multitude of dark patterns implemented by website operators as well as the associated privacy risks highlight the need for further research on how to enable deliberate privacy decisions (e.g., Di Geronimo et al., 2020; Mathur et al., 2019; Nouwens et al., 2020). One possible approach is to examine interventions, which promote *System 2* processing (*educative nudges*). With its exploratory approach, the present study aims to gain insights on one *educative nudge,* in form of a knowledge intervention, and its effectiveness during web cookie privacy decisions, in particular in the presence of dark patterns. Thus, it contributes to present research on educative nudges by incorporating insights from the Dual Process Model and provides first ideas on how educative nudges might be implemented as well as how and which kind of information could be presented. For this approach, participants were instructed to indicate their cookie privacy decision before assessing one cooking webpage to state their first impression (as cover story). The associated knowledge intervention consisted of supporting information on three cookie types (session, third-party, tracking) and optional cookies during the privacy decision, where we systematically varied two aspects in an online experiment: (1) whether participants received supporting information on cookie banners or not in (2) the presence or absence of dark patterns. We examined participants' deliberation on and time required for the cookie decisions as well as their cookie activation.

We expected, that supporting information about cookie banners promotes deliberate decisions while prolonging decision times on cookie options. Derived from the Dual Process Model by Kahneman (2003), dark patterns could influence users' privacy decisions due to automatic *System 1* processing (Bösch et al., 2016). According to this idea, *educative nudges* such as supporting information within a knowledge intervention could help users to counteract dark patterns if they enhance *System 2* processing. Consequently, the impact of dark patterns could be reduced leading to privacy-friendly decisions (Bösch et al., 2016; Sunstein & Reisch, 2019). We expected, that participants are less likely to activate cookies if dark patterns are presented with supporting information than without supporting information. Current research found evidence that users are more likely to activate cookies when dark instead of no patterns were presented (e.g., Machuletz & Böhme, 2020; Nouwens et al., 2020; Utz et al., 2019). However, as *System 2* processing should be accompanied with privacy decisions independent of dark patterns impact (Bösch et al., 2016), we expected the difference in cookie activation between dark and no patterns to be reduced when supporting information is presented.

2. Method

Participants

A total of 207 participants between 18 and 64 years (M = 26.3 years, SD = 7.7) completed the experiment (76 males, 129 females, 2 non-binary). Whether participants received trials with (cookie assistant) or without (app

advertisement) information was randomly assigned between participants resulting in 47.8 % of participants in the "no information" condition and 52.2 % in the "information" condition. With respect to their digital media usage, more than half of all participants (53.1 %) indicated to use digital media more than 40 hours per week. All participants gave informed consent and agreed to data collection and were recruited through e-mail, social media or university mailing lists. Participation was voluntary and without any payment. Psychology students of RWTH Aachen University received course credits for participation. The inclusion criterion was an age of at least 18 years. Data collection was carried out from 7 June to 19 July 2021.

An a-priori power analysis using G*Power Tool (Faul et al., 2007) was conducted to determine the required sample size on the between-subjects comparison between the information and no information groups. For a power of .80 and assuming a medium effect of d =.50 (Cohen, 1988) with an alpha level of α = .05, a total sample size of N = 128 or larger was determined.

Material and apparatus

The experiment was created with PsychoPy 2020.2.10 (Peirce et al., 2019) and hosted on Pavlovia (Bridges et al., 2020). For participation, a laptop or computer with a commonly used browser (Chrome, Edge, Safari, Firefox) was mandatory. Stimuli were centered and adapted to the participants' screen and its size (adaptable size for each stimuli). The stimulus material consisted of 14 mock-up cooking webpages and four—pattern (2) x information (2)—cookie banners per webpage with a screen resolution of 1384 x 1080 Pixel. All resulting 56 cookie banners included a counterbalanced amount of either dark and no patterns as within-subject factor as well as either supporting information via a cookie assistant or no information via an app advertisement as between-subjects factor (see Figure 1 for examples). This resulted in 28 cookie banners with supporting information (cookie assistant) or without information (app advertisement), in which each presented 14 cookie banners with dark and 14 cookie banners with no patterns. Dark patterns were implemented by highlighting only the accept-all button with color whereas no patterns included cookie banners where both (accept/reject) buttons were highlighted with color (i.e., interface interference or aesthetic manipulation; Fansher et al., 2018; Graßl et al., 2021). Additionally, within the information condition, supporting information on three cookie types (session, third-party, tracking) and optional cookies were presented by a cookie assistant whereas, within the no information condition, an app advertisement for the respective website was presented. The cookie information within the information condition was based on the German Consumer Association (Verbraucherzentrale, 2021). Both conditions (information/no information) consisted of an approximately equal number of words as pop-up to the left and above the cookie banner. Additionally, to encourage a deliberate rather than a fear-led decision, fear-inducing language was avoided when designing the information condition (see Figure 1 for examples of stimuli webpages and Appendix A for its English translation). Each cookie banner was presented as a layer above the subsequent website and participants were able to click on the buttons "Disagree to all" or "Agree to all". The subsequent cooking webpages varied for color (green/blue/red/orange/brown/ grey), design ("cooking planet"-"Kochplanet" /"cooking friends"-"Kochfreunde") and recipe (salad/pasta) and were presented once to each participant (independently of their cookie decision). Within the experimental condition, participants' cookie decision (accept/decline) and reaction time were measured. Further, participants' first impression for the cooking webpage on a Likert scale from 1 (terrible) to 7 (very good) and, optionally, one word that describes their first impression were queried (see Appendix B). The first impression task served as a cover story and was not recorded.

Further, demographic data (age, gender), digital-media usage and a post-hoc questionnaire were queried. The post-hoc questionnaire contained questions regarding *deliberation* of the cookie decision and *privacy attitude*. Furthermore, *treatment checks* for the knowledge intervention were included. Both, the experimental phase and the questionnaire, were tested for comprehensibility with three one-on-one tests using think aloud techniques.

Deliberation was measured through six items on a Likert scale from 1 (I do not agree at all) to 7 (I totally agree). As the Dual Process Model distinguishes *System 1* and *System 2* processing (Kahneman, 2003), items related to either intuitive or rational decision-making (see, Hamilton et al., 2016). Two rational and three intuitive items by Hamilton et al. (2016) and one rational item by Graßl et al. (2021) served as template. Both were translated and adapted to cookie decisions. *Privacy attitude* was measured with seven items on a Likert scale from 1 to 7 where each scale's legend varied. Six items by Dienlin and Trepte (2015) on general attitude towards privacy were reformulated for information dissemination via cookie banners and used as templates together with one item by Machuletz and Böhme (2020) on perceived importance. It should be noted that privacy attitude is not reported or included within the results as it does not belong to the reported research question. To verify a knowledge improvement by the cookie assistant in comparison to the app-advertisement (*treatment check*), participants had to examine cookie-statements as true or wrong and identify which cookie banners are mandatory or optional. All questions

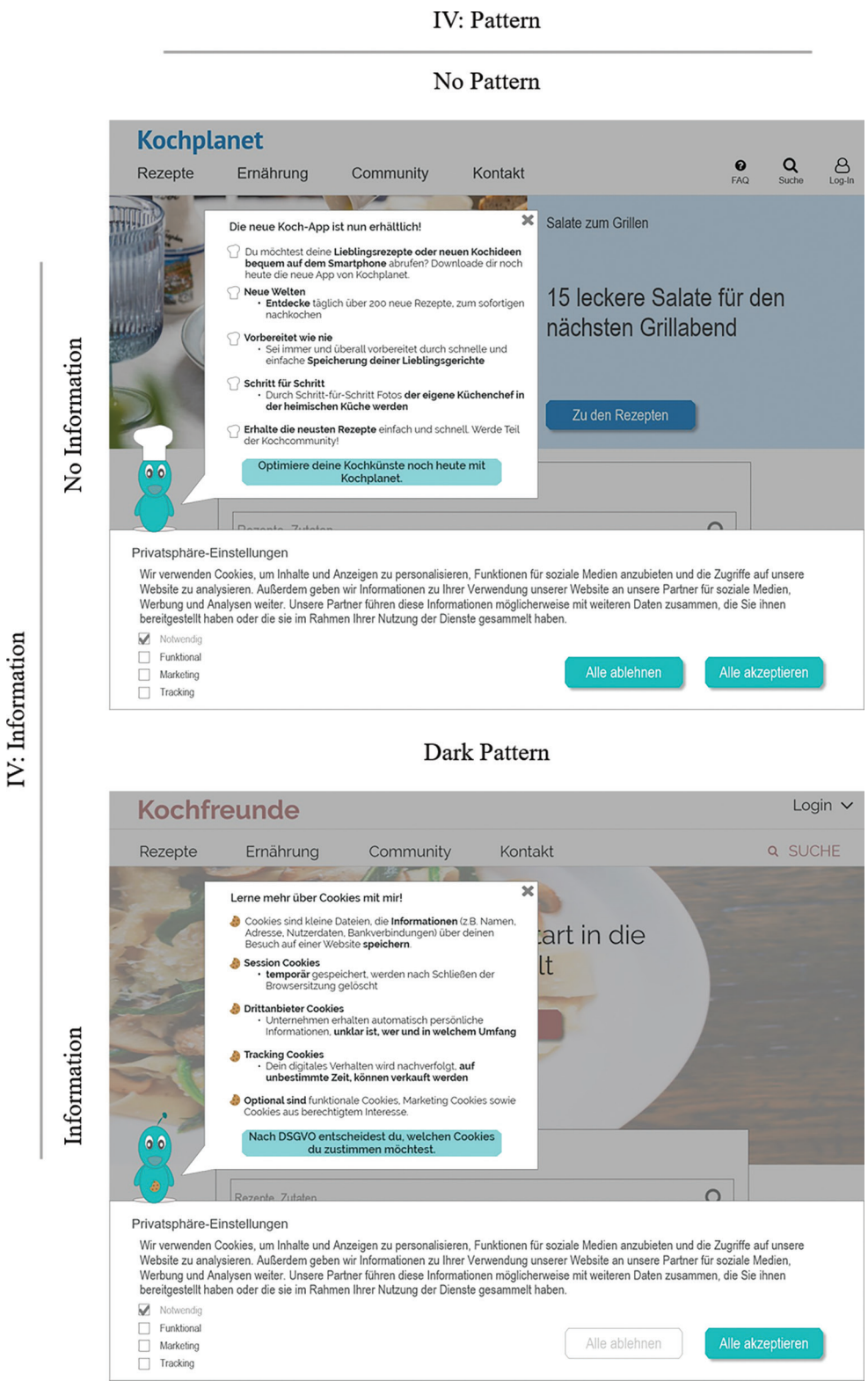


Figure 1. Stimuli examples for no or dark pattern as well as (no) information condition for blue, cooking planet, salad cooking webpage as well as brown, cooking friends, pasta cooking webpage (translations of stimuli webpages for both conditions (no information, information) are provided in Appendix A).

were answerable with the cookie assistant. Further, within the information condition, participants should rate their perception of the cookie assistant and its informational level with two items on a Likert scale from 1 (I do not agree at all) to 7 (I totally agree). The questionnaires used are listed in Appendix B.

Procedure

Participants needed 15 – 20 minutes to complete the experiment. They gave informed consent and agreed to the privacy declaration before participating. After consenting, participants reported their demographic data (age, gender) and digital media usage per week. Then, the experimental phase started. Participants were instructed to either agree or disagree to cookies and, afterwards, rate a website indicating their first impression on a Likert scale from 1 (terrible) to 7 (very good) as well as, optionally, one word that describes their first impression. Before each trial, participants had to click on "Go" (German: "Los") to calibrate the mouse to the screen middle. In each trial, participants were presented, first, a cookie banner until consent or rejection, then, the underlying website for three seconds and, lastly, a questionnaire querying their first impression (see Figure 2). Reaction time (RT) and cookie activation were measured whereas the first impression task was not recorded. In total, 28 cookie banners were randomized presented per participant. To familiarize participants with their tasks, one practice trial was carried out. After completing all trials, the study purpose was queried to identify whether the cover story worked as intended. Then, participants had to rate items on *deliberation* of their cookie decision, their respective knowledge about cookies (*treatment check*) as well as their *privacy attitude* (post-hoc questionnaire). Lastly, participants, in the information condition, were asked to rate their perception of the cookie assistant and its informational level (*treatment check*). Then, within the debriefing, the purpose of the study was disclosed and explained, participants received contact information and could, if desired, obtain the results after data completion.

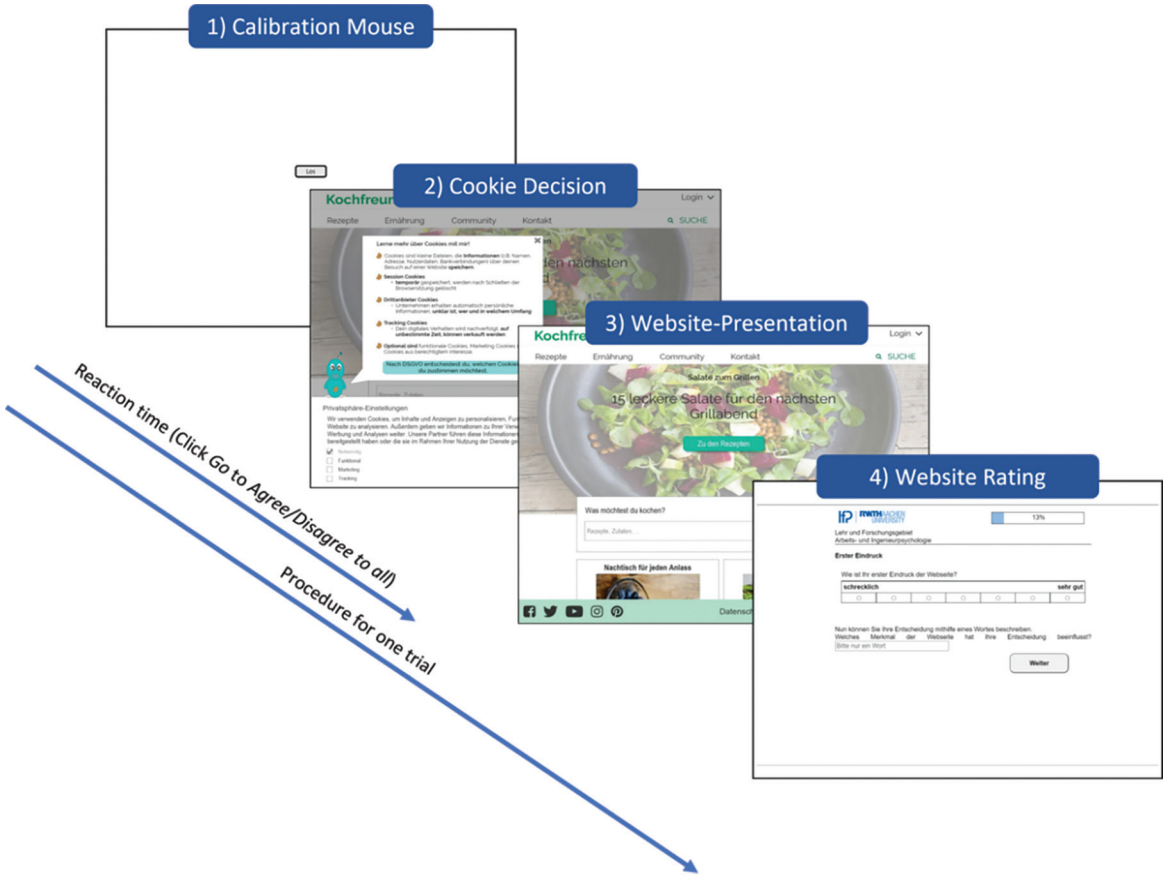


Figure 2. Experimental procedure for one trial representing information condition (cookie-assistant) and cooking webpage (green, cooking friends, salad).

Research ethics

All participants gave written informed consent and participation was voluntary. No undue physical or psychological stress was anticipated as well as participants did not take risks by participating in this study. Participants were able to end data collection at any time and without giving any reason or receiving any disadvantages. Furthermore, participants could skip questions regarding personal information (e.g., age), did not interact with real cookie banners and stimulus material was selected to not raise strong emotions (e.g., fear). Even if, participants were instructed that they should agree or disagree to cookie banners and that their usage behavior will be measured, using the cover story overlaid the full research purpose until the end of the study. However, to enable participants to revoke data storage, data was exclusively saved if participants clicked on "Continue and store data" after debriefing participants about the full research purpose and the applied cover story.

3. Results

For all analyses, the statistic software IBM SPSS Statistics (27.0) with an alpha level of α = .05 was used.

Deliberation and response time

For deliberation and RT analysis, two-sided *t*-tests for independent samples were conducted. Before investigating effects for deliberation, reliability analysis for the deliberation questionnaire was calculated and revealed questionable internal consistency (0.62). Since removing one specific item would not have increased internal consistency, all items were used in the following analysis and classified under this aspect in the discussion. To examine whether participants who received supporting information were more likely to make deliberate decisions on a cookie banner, a two-sided *t*-test for independent samples was conducted. No significant difference between the no information (M = 2.67, SD = 1.21) and the information condition (M = 2.58, SD = 1.12) was found regarding participants' deliberation, $t(205) = 0.61$, $p = .55$, $d = 0.08$.

For RT analysis, RTs were *z*-transformed per participant and trials with *z*-scores of -3/+3 (Field, 2013) as well as trials over 120 seconds served as exclusion criteria. Considering these criteria, a total of 2.8 % trials (164 out of 5796 trials) were excluded from RT analysis. Overall, participants took on average three seconds for a cookie decision (M = 2.90, SD = 3.18). A two-sided *t*-test for independent samples on RTs revealed no significant difference between both information conditions, $t(205) = 1.31$, $p = .19$, $d = 0.18$. Thus, participants, who received supporting information, did not take longer for their decision on a cookie banner (M = 2753 ms, SD = 1716 ms) than participants who did not receive supporting information (M = 3063 ms, SD = 1684 ms). Further, it was examined whether RT was influenced by the presence of dark patterns. However, a 2x2 mixed ANOVA with repeated

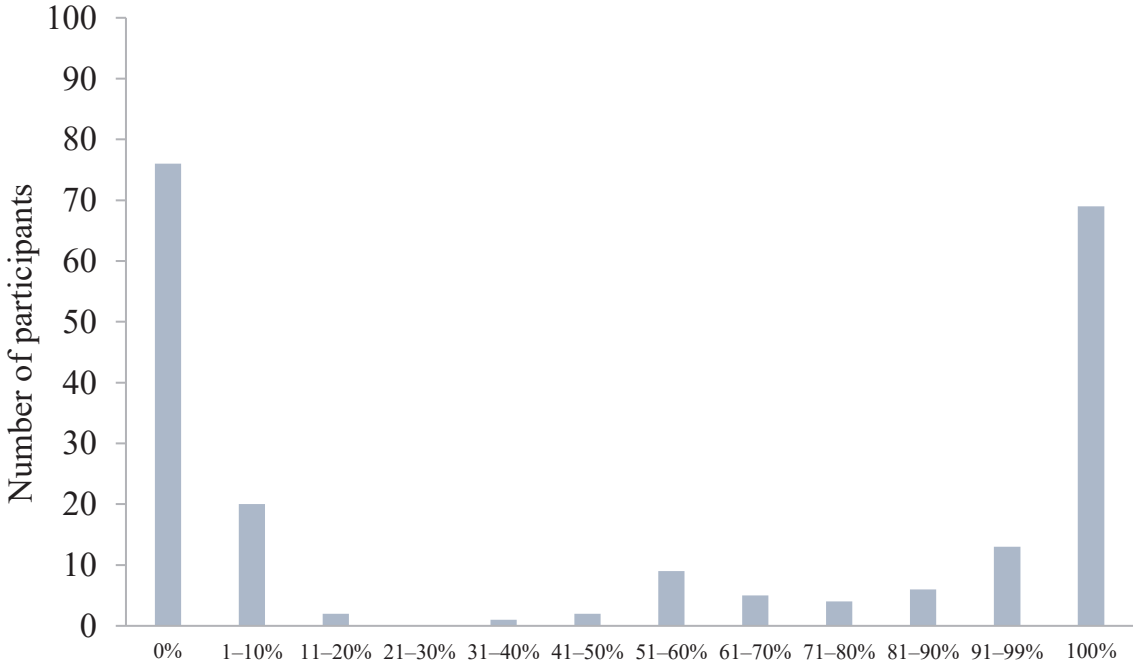


Figure 3. Frequency distribution of participants' cookie acceptance rate across

measures, capturing pattern (dark vs. no pattern) as within-subject factor and information condition (with vs. no information) as between-subjects' factors, did not reveal a significant main effect of pattern on RTs, $F<1$, indicating no dark pattern impact on RT to cookie banners. Further, no main effect of condition nor interaction between condition and pattern was found ($F \leq 1.72$; $p's \geq .19$).

Cookie activation

Before investigating effects on cookie activation, the relative frequency (in %) of cookie activation was averaged across all trials per participant. The frequency distribution (see Figure 3) presented that 36.7 % (N = 76) participants revealed constant cookie rejection behavior (0 % cookie acceptance) and 33.3 % (N = 69) participants revealed constant cookie acceptance behavior (100 % cookie acceptance). In total, this resulted in 70.0 % (N = 145) participants with constant cookie activation behavior. All participants were included in the following analysis. Afterwards, it was analyzed whether cookie activation differs for dark patterns in dependence of their assigned information condition. For trials including dark patterns, a two-sided t-test for independent samples revealed no significant difference in cookie activation when information was presented (M = 52.3 %, SD = 48.1) in comparison to the no information condition (M = 48.3 %, SD = 47.5), $t(205) = -0.60$, $p = .55$, $d = -.08$. Thus, no evidence was found that, in the presence of dark patterns, participants who received supporting information were less susceptible to cookies than participants without assisting information.

Further, it was assumed that cookie activation decreases when supporting information is presented in particular when dark patterns are present. To test this hypothesis, a 2x2 mixed ANOVA, with pattern (dark vs. no pattern) as within-subject factor and information (with vs. no information) as between-subjects factor on cookie activation was calculated. The ANOVA revealed the frequently shown impact of dark patterns on cookie activation, $F(1, 205) = 9.59$, $p < .01$, $\eta_p^2 = .05$. This significant main effect indicates that cookie banners with dark patterns were activated on average in M = 50.4 % (SD = 47.7) of all trials per participant whereas cookie banners with no patterns were only activated on average in M = 46.4 % (SD = 47.0) of all trials per participant. However, there was no significant interaction between pattern and information, $F(1, 205) = 1.06$, $p = .31$, $\eta_p^2 = .01$, and with this no evidence that supporting information reduced the influence of dark patterns on cookie activation (see also Figure 4). Descriptively, the difference even seems to proceed in the opposite direction. Further, no significant main effect for condition was found (no information: M = 46.4%, SD = 47.0; information: M = 50.4, SD = 47.7), $F < 1$.

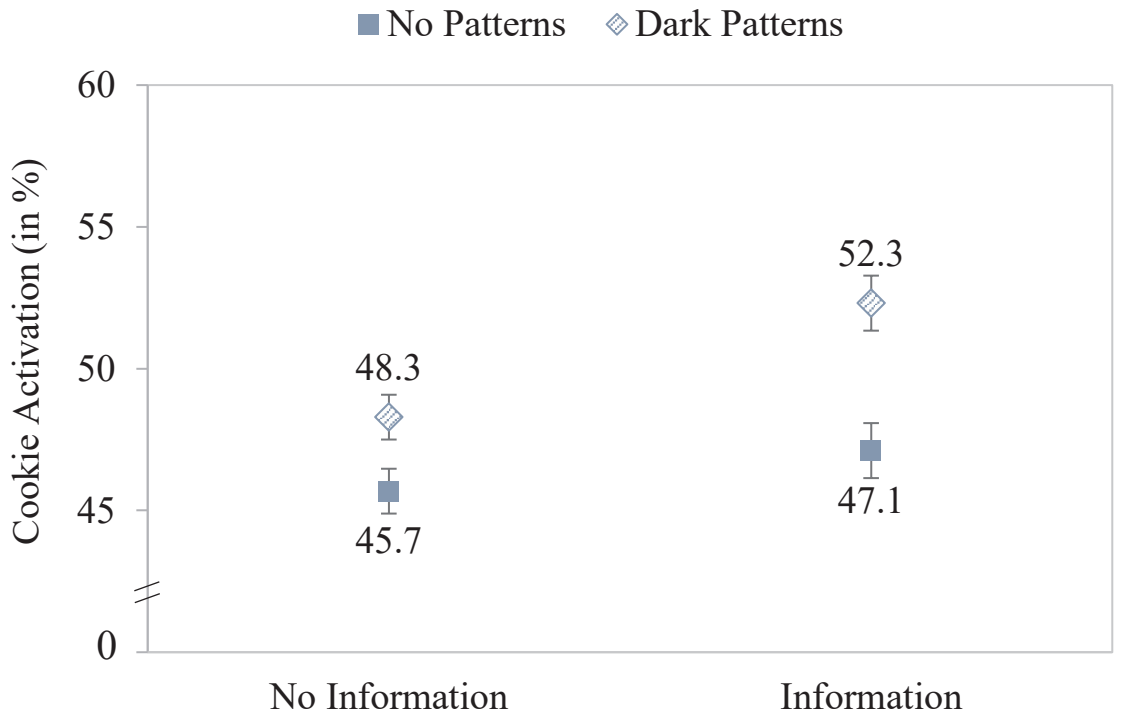


Figure 4. Cookie activation (in %) by information condition (between-subjects) and pattern (within-subject); error bars indicate standard errors within-subject as computed according to Cousineau (2005).

Treatment checks

To identify whether the cover story worked as intended, open answers on study purpose were coded and revealed that 163 participants indicated websites, e.g., its design, as study purpose compared to 41 participants who indicated cookies as study purpose.

To examine if information via the cookie assistant was read, it was analyzed whether participants' knowledge differed between conditions (information vs. no information). In accordance to Strycharz et al. (2021), correct answers were coded as 1 and incorrect answers were coded as 0. The calculated mean represented the knowledge score. However, participants in the information condition (M = 0.68, SD = 0.09) did not have significantly greater knowledge than participants who received no information (M = 0.68, SD = 0.10), $t(205)$ = -0.07, p = .94, d = -.01.

To measure cookie assistance and its informational level, participants' impression of the cookie assistant was recorded with two items (α = .78). Results revealed "medium" consent to the cookie assistants' informational level with M = 3.08 (SD = 1.73) on a scale from 1 (I do not agree at all) to 7 (I totally agree).

4. Discussion

The present online experiment examined the influence of a knowledge intervention and its effectiveness to encourage deliberate privacy decisions when dealing with dark patterns in web cookie banners. Additionally, it was examined whether an increase in users' knowledge can empower them to make privacy-friendly decisions regardless of dark patterns. The empirical findings, however, revealed no evidence for a successful intervention as neither more deliberate and slower nor more privacy-friendly decisions were made when participants received supporting information via a cookie assistant. By integrating current theoretical and empirical findings on dark patterns, the results, potential influencing factors and practical implications are discussed below.

Consonant with various studies (e.g., Machuletz & Böhme, 2020; Nouwens et al., 2020; Utz et al., 2019), we found evidence that dark patterns increased participants' acceptance rate of cookies, underlining their impact on privacy decisions. More important, the present study lends further support to the problematic nature of dark patterns as results demonstrate their resilience against interventions. Focusing on participants' deliberation and time required for cookie decisions, we expected that the knowledge intervention should benefit users' *System 2* processing and encourage their deliberation on and time required for a cookie decision. However, no evidence was found in this respect. On the contrary, independent of whether or not cookie assistance was given, participants had low to medium deliberation scores and made fast cookie decisions. Consistent with the findings on reaction time and deliberation, but contrary to our expectations, no impact of the given information on cookie activation in general nor on the influence of dark patterns was given. However, it should be noted that the majority of our participants (about 70 %) showed constant cookie related behavior, i.e. they either accepted or rejected all cookies. This might be an indicator for previously defined cookie strategies or conditioned behavior. Overall, no evidence was found that the developed knowledge intervention promoted users' deliberate *System 2* processing or enhanced users' ability to counteract dark patterns. Even if the informational level of the cookie assistant revealed medium scores and the cover story worked as intended (163 participants indicated the websites as study purpose), these results and similar knowledge scores between both conditions demonstrated that the implemented knowledge intervention did not work as intended.

One reason could be, that the present study conveys unsuitable information or fails to convey information at all. As the knowledge intervention referred to topic-relevant knowledge, we believe that the information itself should have been able to increase users' performance on the knowledge questions, especially since the fit between its content and the control questions was large. In contrast to this expectation, the subsequent questionnaire did not show differences in participants' knowledge level between participants who received the information and those who did not. This might indicate, that the former participants might have ignored the information because it lacked visual salience, was too extensive or they wanted to get rid of it as quickly as possible to return to the primary task: rating the webpages. As mentioned above, users in *System 1* processing do not deliberate their decision and tend to focus on the highlighted and simplest option, which is one reason why dark pattern work as intended (Bösch et al., 2016). However, the present results demonstrate how difficult it is to lead users to *System 2* processing in the first place and knowledge interventions alone might not be the right tool to combat highly automated behavior such as clicking on cookie banners. Other visualizations for knowledge interventions must be considered that have higher visual salience and are able to grab users' attention even under these difficult circumstances. To achieve this goal, the intervention should "pop-out", e.g. by using vivid and high contrast colors or animations. It also has to be visually different from irrelevant information, for example adds, so that the intervention is not mistaken as distractor. One approach could be to integrate *privacy-by-design* approaches (e.g., Barth et al., 2021) and present privacy locks above the cookie buttons or information presented right above the cookie banner.

As about 70 % of the participants revealed constant response behavior, it could be argued that participants developed strongly conditioned behavior on cookie requests over time. The

important role of conditioned behavior is also highlighted by Graßl et al. (2021) who found indications that users developed accepting default behavior on cookie banners independent of dark patterns. Such highly conditioned behavior raises the question whether knowledge interventions alone can be effective, as users must overcome their conditioned behavior to interact with knowledge interventions. As motivation is described as one critical factor to trigger *System 2* processing (Bösch et al., 2016; Brough & Martin, 2020; Terpstra et al., 2019) or to change users' behavior in general (Fogg, 2009), Brough and Martin (2020), for example, argue that knowledge differences need to be combined with motivation to influence users' privacy behavior (see also Fogg, 2009; Terpstra et al., 2019). To encourage users' privacy decisions, Terpstra et al. (2019) further claim that three components must be fulfilled: (1) an interruption of the user's task or goal, (2) an explanation on, e.g., how and why data is stored, and (3) the option to make own choices. Although participants received supporting information to indicate how data is stored and the ability to make their own cookie decisions in the present study, the missing effectiveness of the knowledge intervention could be reasoned in conditioned behavior that cannot be conquered due to insufficient motivation or stimulation (e.g. through an interruption) to engage in reflective thinking. To test this assumption, follow-up investigations could examine whether inquiries (e.g., "Are you sure you want your privacy settings to be saved?") (Terpstra et al., 2019), precise risk communication (e.g. specific risk scenarios, Gerber et al., 2019) or fear appeals (Brough & Martin, 2020; Distler et al., 2020; Harbach et al., 2014) in combination with knowledge interventions could raise awareness and trigger users' *System 2* processing. As some participants who focused on the cover story (website ratings) indicated that the study increased their motivation to change cookie decisions or to learn more about cookies, it could further be examined whether induced discrepancies between users' attitude and behavior could improve motivation for privacy decisions.

Limitations

Besides these alternative explanations and research suggestions, the given results should be considered in view of potential methodological limitations. First, it could be argued that the knowledge intervention did not show the desired effects as the research context provided a certain level of security. Rather than showing their regular privacy behavior, the resulting feeling of safety in the context of a scientific experiment could provoke participants to mainly focus on the primary task (rating websites). However, as participants used their own devices, and as it was not indicated that faked cookies were used until the end of the experiment, this alternative explanation cannot fully explain the results. Moreover, it cannot be ruled out that the present study showed too little internal consistency in the deliberation questionnaire. However, as no effect of the knowledge intervention was found on RT or cookie activation as well as the majority of our participants showed constant cookie related behavior, these methodological limitations do not seem to strongly affect the present results.

Practical implications

As results indicate that participants made highly conditioned, undeliberated, and fast decisions on the ubiquitous consent requests of cookie banners, the question arises whether state-of-the-art repetitive cookie requests are purposeful. Even if the GDPR attempts to provide users' with "freely given, specific, informed and unambiguous" (GDPR, 2016, p. 6) privacy decisions, the resulting repetitive cookie requests could be associated to conditioned rather than informed privacy decisions (see, Graßl et al., 2021). Such results underline the importance of new legal developments such as *PIMS* (*P*ersonal *I*nformation *M*anagement *S*ystems), where users declare their consent once and website operators will be informed on their consent (see also, John & Rennert, 2022). Such one-time privacy decisions could reduce the effort required and increase users' motivation to deliberately decide on their privacy settings. As website operators would still be entitled to request individual and customizable privacy decisions under the new legislation (see also, John & Rennert, 2022), it should be ensured that these customizable cookie decisions will not be enforced to visit a website or connected to dark patterns in order to gain users' data.

Further, the present study indicates that participants lacked the knowledge to make privacy decisions on cookie requests. These insights into users' cookie decisions highlight the need for an increase of users' knowledge on privacy and cookie requests. Hence, legal regulations should not only ensure informative and easily understandable consent requests through *educative nudges* (Sunstein & Reisch, 2019) but also improve users' digital literacy with specific trainings (*long-term boosts*) (Hertwig & Grüne-Yanoff, 2017). Further trainings (*long-term boosts*) on, e.g., users' digital literacy could be developed as educational measure. For example, app-based privacy trainings (e.g. FoxIt; Gerber et al., 2018) or serious games (as developed, for example, within the project A-DigiKomp: https://www.a-digikomp.rwth-aachen.de) might be suitable to playfully improve digital literacy.

Conclusion

By demonstrating that participants make undeliberated, fast as well as privacy-unfriendly decisions regardless of supporting information, the present results question the effectiveness of, so far, implemented consent requests on cookie banners and the presented knowledge intervention. As users seem to develop highly conditioned behavior on

repetitive privacy decisions, we argue for a reformation of current cookie requests in particular and more research on privacy-enhancing interventions by taking simplified knowledge as well as motivation into account.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274. https://doi.org/10.1086/671754

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Barth, S., Ionita, D., De Jong, M. D., Hartel, P. H., & Junger, M. (2021). Privacy rating: a user-centered approach for visualizing data handling practices of online services. *IEEE transactions on professional communication*, *64*(4), 354–373. https://doi.org/10.1109/TPC.2021.3110617

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021). "I am definitely manipulated, even when I am aware of it. It's ridiculous!" – Dark patterns from the end-user perspective. In W. Ju, L. Oehlberg, S. Follmer, S. Fox, S. Kuznetsov (Eds.), *Designing Interactive Systems Conference 2021 (DIS'21)* (pp. 763–776). Association for Computing Machinery. https://doi.org/10.1145/3461778.3462086

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, *2016*(4), 237–254. https://doi.org/10.1515/popets-2016-0038

Bridges, D., Pitiot, A., MacAskill, M. R., & Peirce, J. W. (2020). The timing mega-study: Comparing a range of experiment generators, both lab-based and online. *PeerJ*, *8*, e9414. https://doi.org/10.7717/peerj.9414

Brough, A. R., & Martin K. D. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology*, *31*, 11-15. https://doi.org/10.1016/j.copsyc.2019.06.021

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed). Lawrence Erlbaum Associates.

Cousineau, D. (2005). Confidence intervals in within-subject designs: A simpler solution to Loftus and Masson's method. *Tutorials in Quantitative Methods for Psychology*, *1*(1), 42–45. https://doi.org/10.20982/tqmp.01.1.p042

Culnan, M. J., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104

Dennis, A. R., & Minas, R. K. (2018). Security on autopilot: Why current security theories hijack our thinking and lead us astray. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *49*(SI), 15–38. https://doi.org/10.1145/3210530.3210533

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)* (pp. 1–14). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376600

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Distler, V., Lenzini, G., Lallemand, C., & Koenig, V. (2020). The framework of security-enhancing friction: How UX can help users behave more securely. In *New Security Paradigms Workshop 2020 (NSPW '20)* (pp. 45–58). Association for Computing Machinery. https://doi.org/10.1145/3442167.3442173

Fansher, M., Chivukula, S. S., & Gray, C. M. (2018). #darkpatterns: UX practitioner conversations about ethical design. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)* (pp. 1–6). Association for Computing Machinery. https://doi.org/10.1145/3170427.3188553

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*, 175–191. https://doi.org/10.3758/BF03193146

Field, A. (2013). *Discovering statistics using IBM SPSS statistics.* (3rd ed.). Sage.

Fogg, B. J. (2009). A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology (Persuasive '09)* (pp. 1–7). Association for Computing Machinery. https://doi.org/10.1145/1541948.1541999

General Data Protection Regulation (GDPR) (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE

Gerber, N., Reinheimer, B., & Volkamer, M. (2019). Investigating People's Privacy Risk Perception. *Proceedings on Privacy Enhancing Technologies*, 2019(3), 267-288. https://doi.org/10.2478/popets-2019-0047

Gerber, N., Gerber, P., Drews, H., Kirchner, E., Schlegel, N., Schmidt, T., & Scholz, L. (2018). FoxIT: enhancing mobile users' privacy behavior by increasing knowledge and awareness. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust* (pp. 53-63).

Graßl, P., Schraffenberger, H., Borgesius, F. Z., & Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, *3*(1), 1–38. https://doi.org/10.31234/osf.io/gqs5h

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)* (pp. 1–14). Association for Computing Machinery. https://doi.org/10.1145/3173574.3174108

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05)* (pp. 71–80). Association for Computing Machinery. https://doi.org/10.1145/1102199.1102214

Hamilton, K., Shih, S.-I., & Mohammed, S. (2016). The development and validation of the rational and intuitive decision styles scale. *Journal of Personality Assessment*, *98*(5), 523–535. https://doi.org/10.1080/00223891.2015.1132426

Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014). Using personal examples to improve risk communication for security and privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems (CHI '14)* (pp. 2647–2656). Association for Computing Machinery. https://doi.org/10.1145/2556288.2556978

Hertwig, R., & Grüne-Yanoff, T. (2017). Nudging and boosting: Steering or empowering good decisions. *Perspectives on Psychological Science*, *12*(6), 973–986. https://doi.org/10.1177/1745691617702496

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. *American Economic Review*, *93*(5), 1449–1475. https://doi.org/10.1257/000282803322655392

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Machuletz, D., & Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), 481–498. https://doi.org/10.2478/popets-2020-0037

Maier, M., & Harr, R. (2020). Dark design patterns: An end-user perspective. *Human Technology*, *16*(2), 170–199. https://doi.org/10.17011/ht/urn.202008245641

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–32. https://doi.org/10.1145/3359183

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What makes a dark pattern... dark?: Design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)* (pp. 1–18). Association for Computing Machinery. https://doi.org/10.1145/3411764.3445610

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)* (pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376321

Peirce, J., Gray, J. R., Simpson, S., MacAskill, M., Höchenberger, R., Sogo, H., Kastman, E., & Lindeløv, J. K. (2019). PsychoPy2: Experiments in behavior made easy. *Behavior Research Methods*, *51*, 195–203. https://doi.org/10.3758/s13428-018-01193-y

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). Can I opt out yet?: GDPR and the global illusion of cookie control. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19)* (pp. 340–351). Association for Computing Machinery. https://doi.org/10.1145/3321705.3329806

Strycharz, J., Smit, E., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, *120*, 106750. https://doi.org/10.1016/j.chb.2021.106750

Sunstein, C. R. (2016). *The ethics of influence: Government in the age of behavioral science*. Cambridge University Press. https://doi.org/10.1017/CBO9781316493021

Sunstein, C. R., & Reisch, L. A. (2019). Educative nudges and noneducative nudges. In C. R. Sunstein & L. A. Reisch (Eds.) *Trusting Nudges* (1st ed., pp. 95-118). Routledge. https://doi.org/10.4324/9780429451645

Terpstra, A., Schouten, A. P., de Rooij, A., & Leenes, R. E. (2019). Improving privacy choice through design: How designing for reflection could support privacy self-management. *First Monday*, *24*(7), 1–19. https://doi.org/10.5210/fm.v24i7.9358

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)* (pp. 973–990). Association for Computing Machinery. https://doi.org/10.1145/3319535.3354212

Verbraucherzentrale. (2021). *Cookies kontrollieren und verwalten*. Verbraucherzentrale.de. https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/cookies-kontrollieren-und-verwalten-11996.

Appendix A

Information text (translated to English)

Table Appendix A:

Condition	Information text	Source
Information (Cookie Assistant)	Learn about cookies with me! – Cookies are small files that *store information* (e.g. name, address, user data, bank details) about your visit on a website. – **Session cookies** ○ **Temporarily** stored, are deleted after closing the browser session – **Third party cookies** ○ Companies automatically receive personal information, it is unclear who and to what extent – **Tracking cookies** ○ Your digital behavior is tracked, for an **indefinite period, can be sold** – **Optional are** functional cookies, marketing cookies and cookies for legitimate interest. According to DSGVO, you decide to which cookies you want to agree.	The cookie information was based on the German Consumer Association (Verbraucherzentrale, 2021)
No Information (App Advertisment)	The new cooking app is now available! – You want to access your f**avorite recipes or new cooking ideas conveniently on your smartphone?** Download the new app from Kochplanet/Kochfreude today. – **New worlds** ○ **Discover** over 200 new recipes every day for instant re-cooking – **Prepared as never before** ○ Be prepared anytime, anywhere with quick and easy **storage of your favorite dishes** – **Step by step** ○ **Become your own chef in the home kitchen** through step-by-step photos – **Get the newest recipes** easily and quickly. Become part of the cooking community! Optimize your cooking skills today with Kochplanet/Kochfreunde.	

Appendix B

Questionnaires (translated to English)

Table Appendix B:

Variable	Measurement Item	Source
First impression	*[Likert scale, (1) terrible to (7) very good; open answer]* – What is your first impression of the website? – optional: What feature of the website influenced your decision?	
Study purpose	*[open answer]* – What do you think this study is about?	
Deliberation	*[Likert scale, (1) I do not agree at all to (7) I totally agree]* – Before selecting a cookie option, I considered all possible cookie options. – Before choosing a cookie option, I took time to weigh the advantages and disadvantages of my decision. – Before selecting a cookie option, I carefully read the cookie policy. – I intuitively selected a cookie option. – I selected the cookie option, which corresponds to my first impression. – I trusted in my feeling when I chose a cookie option.	Hamilton et al. (2016) Graßl et al. (2021) served as template
Knowledge	*[single choice; true, wrong]* Cookies are … … security patches designed to close security issues on the computer. … text information that is stored on a device when a website is visited. … another word for privacy policies. Session cookies… … are deleted after each browser session. … are stored temporarily. … automatically share personal information with other companies. … can be sold to other companies. … can store digital behavior over multiple browser sessions. Third party cookies… … are deleted after each browser session.	Encoding was adopted from Strycharz et al. (2021) Cookie information was based on Verbraucherzentrale (2021)
Knowledge	… are stored temporarily. … automatically share personal information with other companies. … can be sold to other companies. … can store digital behavior over multiple browser sessions. Tracking cookies… … are deleted after each browser session. … are stored temporarily. … automatically share personal information with other companies. … can be sold to other companies. … can store digital behavior over multiple browser sessions. What types of cookies are optional? … necessary cookies … functional cookies … marketing cookies … cookies for legitimate interest	Encoding was adopted from Strycharz et al. (2021) Cookie information was based on Verbraucherzentrale (2021)
Privacy Attitude	*[Likert scale; 1 to 7, alternating response format]* I think that sharing personal information via cookies on a website ... … is not meaningful (1) to meaningful (7). … is disadvantageous (1) to advantageous (7). … is questionable (1) to harmless (7). … is dangerous (1) to not dangerous (7). … is reckless (1) to deliberate (7). … is bad (1) to good (7). The protection of my privacy on the Internet is... … unimportant (1) to important (7).	Dienlin and Trepte (2015) Machuletz and Böhme (2020) served as template
Cookie Assistant	*[Likert scale, (1) I do not agree at all to (7) I totally agree]* – The Privacy Assistant helped me to select a cookie option. – Through the Privacy Assistant, I have received helpful information on the subject of cookies.	