usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

# Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect

Agnieszka Kitkowska, *Karlstad University;* Mark Warner, *Northumbria University;* Yefim Shulman, *Tel Aviv University;* Erik Wästlund and Leonardo A. Martucci, *Karlstad University*

https://www.usenix.org/conference/soups2020/presentation/kitkowska

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

# Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect

Agnieszka Kitkowska
*Karlstad University*

Mark Warner
*Northumbria University*

Yefim Shulman
*Tel Aviv University*

Erik Wästlund
*Karlstad University*

Leonardo A. Martucci
*Karlstad University*

## Abstract

When people sign-up to new online services, privacy notices are the initial means by which data handling practices are communicated. Yet, their design seldom ensures users' privacy comprehension or provides people with privacy choices, resulting in negative feelings associated with the sign-up process. In this paper, we investigate how to improve privacy notice design to enhance privacy comprehension and control, while inducing more positive feelings towards these notices. In an online experiment ($N = 620$), we examine the factors of curiosity, privacy concerns, trust, and time. We study how these factors and visual designs of notices (framing and control) influence privacy comprehension, intention to disclose, and affect (negative-positive). Our results show that, depending on an individual's level of curiosity, control can influence privacy comprehension, disclosure, and affect. We demonstrate that affect moderates the relationship between privacy concerns and disclosure. We elaborate on our results, highlighting how privacy notices that activate curiosity and provide control, could enhance usability and strengthen privacy-conscious behaviors.

## 1 Introduction

Privacy issues are on the rise since people's daily activities have become increasingly reliant on internet-connected applications. Such accelerating technological dependency may increase personal information disclosure and data collection; furthermore, it can put people's privacy at risks resulting in harms to individuals [61]. Privacy breaches have been often reported in the media (e.g., [22, 29]), and people became concerned about their online information and how they lack control over its use [17].

Regardless of their concerns people are often required to sign-up to new online applications in order to gain access to services. During the application sign-up process people have to make one of the first decisions about their online privacy, seldom provided with a choice to restrict their disclosures. Moreover, privacy is a complex and context-dependent notion [49], and people may disregard it. Without sufficient understanding and control around personal information during the application sign-up process people's decisions around information disclosure may not be informed or rational. Moreover, they may result in behaviors which contradict the privacy beliefs of individuals.

Policymakers try to improve this by enacting data protection regulations, e.g., the EU General Data Protection Regulation (GDPR) [16], or the California Consumer Privacy Act (CCPA) [7]. These require companies to provide users with adequate information to promote informed consent. Yet, little change has been applied in the visual display of privacy notices communicating data handling practices.

To address this, the research presented in this paper focuses on the visual display of privacy notices. We investigate ways of encouraging users to make more informed privacy decisions which are aligned with their beliefs. We examine the role of framing and control within the design of privacy notices as they have been previously shown to influence privacy decision-making [2, 5, 23]. We also draw on prior work [13], to understand how affective state (negative-positive valence), as well as stable factors (curiosity, privacy concerns, trust) influence privacy interactions. We explore how these factors affect privacy comprehension and intention to disclose.

This work has two main contributions. First, our findings demonstrate that providing users with control can lead to more privacy-aware information disclosures. However, control by itself may be insufficient, as curiosity influences the relationship between control and disclosure. Control may also have an effect on users' affective state (valence). Therefore, we

*USENIX Symposium on Usable Privacy and Security (SOUPS)* 2020.
August 9–11, 2020, Virtual Conference.

propose incorporating methods to enhance both control and curiosity in the design of privacy notices. Such designs have the potential to improve privacy and disclosure decisions during the application sign-up process, as well as lead to better usability through elevated levels of user satisfaction.

Second, our research contributes to the body of knowledge on privacy decisions. We demonstrate that affective state (valence) can moderate the relationship between trust and privacy concerns and, as a result, indirectly affect information disclosure. Such knowledge can be used in future experimental designs and studies modeling privacy decisions.

## 2 Background

To clarify our motivations and introduce our research questions, in this section we present past theoretical and empirical research fundamental for our work.

One of the frameworks explaining the relationships between different factors influencing privacy-related decisions is the APCO model (Antecedents→Privacy Concerns→Outcomes) [13]. We utilize this framework as it is comprehensive, and draws upon previous multidisciplinary research on privacy; the proposed model conceptualizes factors that influence outcomes of privacy decisions. Among the elements incorporated in the APCO model are antecedents of privacy concerns, such as individual characteristics; next, in the centre of the framework is the relationship between trust and privacy concerns; the central part of the model relates directly to behavioral outcomes (e.g., disclosure). The recent revision of the APCO model broadened its scope, and incorporated the level of effort that may be influenced by mental shortcuts and heuristics (e.g., affect). The level of effort relates to dual-process theories, wherein cognition contains two types of processing [18]. Type 1 is low-effort, fast, automatic, and relies on pre-existing mental models and experiences. Type 2 requires high levels of cognitive effort, is less automatic and therefore, a slower form of cognitive processing.

The current research investigates the relationships between the factors mentioned above, which relate to the low-effort, Type 1 cognitive processing. We examine them in the context of two outcome variables: privacy comprehension and intention to disclose. Further, we study the effect that external factors—framing and control—might have on these outcome variables.

### 2.1 APCO factors

In the APCO model, information disclosure is one of the behavioral outcomes of privacy decision-making. As demonstrated in the meta-review by Gerber et al. [21] privacy concerns and trust can be predictors of intention to disclose. The APCO framework also proposes that affect might have a moderating role in the relationship between attitudes and behavior, and that individual characteristics might have an indirect effect on behavioral outcomes.

#### 2.1.1 Privacy Concerns

Privacy concerns are considered an attitudinal factor influencing decision-making, and they were investigated in many studies (e.g., [13, 60]). Some of the studies focusing on privacy concerns addressed the *privacy paradox*, meaning the phenomenon when people may express high levels of privacy concerns whilst also tending to over-disclose their personal information [6,51]. However, the findings of the *privacy paradox* research are inconclusive. In one study privacy-concerned people were found to disclose less [14], whilst in another study, this finding existed only under certain conditions, e.g., when perceived damage and enjoyment might have altered the relationship between concerns and disclosure [10]. On the other hand, Taddicken [65], in the context of the social web, found privacy concerns having little to no effect on self-disclosure.

#### 2.1.2 Trust

Past research has shown that people use trust beliefs in the decision-making process around information disclosure [39]. Trust has primarily been found influential when the decision is made under uncertainty, as is frequently the case when people make decisions around online privacy [53]. Trust may also influence "rationally" calculated privacy decisions, e.g., users involve their trust beliefs in the context of sensitive information disclosure [10]. Visual cues might alter trust, e.g., in their study, Zhang et al. [71] showed that cues displaying "instant gratification" (financial reward for registration) decreased trust towards a website. On the other hand, visual cues granting control over the information, combined with salient information about how data might be used for advertisement, were found to increase trust towards the application provider [69]. Consequently, such cues seemed to positively impact the willingness to install applications, which could result in increased information disclosure.

#### 2.1.3 Affective state

Decisions around privacy have also been investigated through the lens of biases and heuristics that may take over the rational, in an economic sense, decision-making. One of the approaches explaining the "irrational" decisions is the affect heuristic related to information processing. There is not much of a consensus about the definition of affect, and the current work follows the description from Lerner: "the superordinate umbrella of constructs that involves emotion, mood, and emotion-related traits" [42, p. 801]. Further, we recognize the circumplex components of affect: valence (positive-negative) and arousal (high-low) [55].

According to the affect heuristic, people add either positive or negative value to their decision outcome [20]. The affect-as-information hypothesis postulates that emotions are felt, and this feeling has a significant impact on cognitive processing, providing conscious information from unconscious appraisal situations [9]. These feelings can guide immediate actions. Similarly, the feelings-as-information theory proposes that positive affect indicates if a given situation is safe [58]. Negative affect signifies that a situation is unsafe, and more cognitive processing is needed. Therefore, positive affect may serve as an incentive to rely on internal thoughts and inclinations, whereas negative affect should direct attention to new, external information. The affect may be elicited by an external stimulus, such as the way information is presented or semantic context, in which the situation takes place [58].

In the context of privacy, affect has been shown to shape risk perceptions [38]. It has a lasting consequence on privacy beliefs, e.g., in an e-commerce environment [43]. Further, negative valence may increase privacy attitude and decrease sharing, while positive valence may increase sharing attitude and decrease privacy attitude [11]. In the current work, we want to further investigate the affect by asking the following research questions:

**RQ1** Does the visual design of privacy notices (framing and control) influence affective state?

**RQ2** What is the role of the affective state (if any) in the relationship between attitudinal factors and intention to disclose?

### 2.1.4 Individual characteristics: curiosity

In psychology and behavioral research, curiosity is regarded as one of the stable personality characteristics that drive how people perceive the world, and how they make judgements and decisions [44]. To the best of our knowledge, not much of attention has been given to curiosity in privacy research. Curiosity is closely related to learning and knowledge acquisition. Information-gap-theory proposes that curiosity is "arising when attention becomes focused on a gap in one's knowledge" [44, p. 87]. In consequence, it makes an individual curious and motivates them to seek more information. Hence, curiosity may play the role of a marker, the reference point that encourages an individual to obtain more information. Curiosity might be stimulated by external factors and reduce uncertainty about current circumstances [24, 44].

Considering scarce research about the interplay of curiosity and privacy interactions, we raise the following research question:

**RQ3** Does curiosity influence privacy comprehension?

## 2.2 External factors

Past work investigated privacy comprehension in many contexts, e.g., mobile permission warnings, data visualizations, end-user licence agreements [19, 36, 68]. The results showed that visual representation might impact comprehension. For instance, supplementary information may lead to a higher understanding of data collection practices [14]. Further, the visual cues with salient privacy information can not only improve understanding and increase privacy awareness, but also enhance management of privacy permissions and influence information disclosure [38].

### 2.2.1 Framing

One of the approaches applied to investigate privacy interactions is framing, meaning that the frame of a decision is designed in a way that constrains how the problem is presented to the decision-maker [47]. Such framing is expected to influence the decision outcome. The framing was used to improve risk communication, and help with pro-privacy decisions (e.g., choice of application, protective attitudes and behaviors) [2, 54]. Furthermore, positive framing successfully nudged users towards less privacy-invasive actions [8]. Emotion eliciting images were shown to influence decisions: the more affective the images, the more weight was placed on impression formation and decision-making [59].

### 2.2.2 Elements of visual design

Studies demonstrated that visual stimuli might influence memory, when they incorporate animations, anthropomorphic designs, clear layouts, such as division into columns [63, 66]. In the context of privacy, research revealed that the end-user agreements presented in abbreviated style, divided into short sections, elicited positive attitudes, increasing comprehension and time of exposure [68].

Past work suggests that text insufficiently communicates privacy information, and other approaches are required to enhance usability [3]. Nevertheless, visual design needs to be carefully crafted to avoid the effects of cluttered or oversymbolic representations. Anthropomorphic designs were shown to increase personal information disclosure [4, 48]. Moreover, comic strips were found to enhance users' attention [64]. Comics may trigger emotions, enabling a greater understanding of the displayed issues [50].

### 2.2.3 Control over information disclosure

Prior research suggests that people want to have control over their personal information [5,38]. Therefore, some researchers provided participants with control and investigated whether it influenced disclosure. The results revealed that control may not necessarily lead to a decrease in information disclosure [5].

People appeared to alter their willingness to disclose in response to non-normative factors (control over publishing their data), but failed to change their behavior in response to the normative factors (e.g., personal identification). As mentioned above, control embedded in visual design, supported by salient information may result in a decrease in disclosing behavior, depending on the context [69].

Considering the effects of visual design on privacy comprehension and information disclosure, in the current work, we want to investigate such a relationship further. Mainly, we aim to examine the role of visual design that incorporates framing and control, in the context of interaction with privacy notices. Therefore, we propose the following research questions:

**RQ4** Does visual design of privacy notices (framing and control) affect comprehension?

**RQ5** Does visual design of privacy notices (framing and control) affect intention to disclose information?

## 3 Method

To answer our research questions we designed an online experiment. The experiment aimed to elicit affective states through framing and control applied in the visual design of privacy notices. The experiment contained four phases: entry questionnaires, interactive application sign-up task, measurement of outcome variables, and exit questionnaires (Figure 1).

Our experiment was designed drawing on findings from prior exploratory studies, which we discuss first.

### 3.1 Exploratory studies

Two exploratory studies preceded the current research, and were used to inform the current study design. Both exploratory studies used freely available platforms to recruit participants, such as the Reddit r/SampleSize.

In the first exploratory study (ST1) [37], we examined why people agree or disagree with privacy notices, and whether the framing of the notice's design elicits changes in affective state. To frame these privacy notices, we used positive and negative anthropomorphic or human-like illustrations. Based on responses from 88 participants, we found that people lack control when acknowledging notices, feeling that they have no other choice but to agree. Drawing on this finding, in the current study, we investigate the effect of control on privacy interactions.

Further, the results of ST1 showed that notice's design alters affect. However, we identified that the framing effects differ, depending on the use of anthropomorphic or human-like illustrations. To clarify the framing effects around these illustrations, we ran the second exploratory study. The study had 36 participants, and each participant was shown 16 images: eight positively and eight negatively framed. Framing groups contained four anthropomorphic and four human-like illustrations, each. The images were arranged in a randomized sequence, and participants were asked to state what feelings they associated with each illustration. We assessed feelings through an instrument similar to the 2D EmojiGrid [67], scoring from 1 (negative) to 5 (positive). For the current study, we chose the positive and negative anthropomorphic representations, because they had the highest and lowest means, respectively (Table 1).

Table 1: Means and standard deviations for positive and negative framing from the second exploratory study (sorted by means, descending).

| Illustration, and framing type | M | SD |
|---|---|---|
| Anthropomorphic, positive | 2.69 | 0.85 |
| Human, positive | 2.52 | 0.79 |
| Human, negative | 2.35 | 0.69 |
| Anthropomorphic, negative | 2.28 | 0.77 |

### 3.2 Main study

In the main study, we applied a $2 \times 2$ between-group design. The between-group variables were (1) framing and (2) control. Further, we measured the constructs presented in Figure 1.

#### 3.2.1 Variables

Framing (positive vs negative), and control (present vs absent) were our independent variables, manipulated between groups. Reported curiosity level of participants (high, low) was also included as an independent variable, but was not manipulated. Outcome variables were post-stimulus measurements of affect, intention to disclose, and privacy comprehension.

We included covariates (privacy concerns, trust, approximate time spent on the notice page, and pre-stimulus affective state) to control for their influence on the dependent variables.

#### 3.2.2 Ethical review

The experimental design underwent an ethical review from the Karlstad University Ethical Review Board. The review board determined that this work would not expose participants to any undue risk. To comply with the legal requirements, the researchers made an effort to minimize data collection and reduce the probability of identifying an individual. No personal information was requested from the participants. However, where participants identified themselves (e.g., sent an email), their data was anonymized after the data collection had been completed.

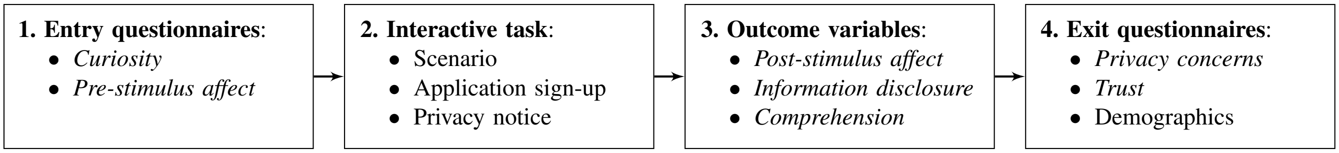


Figure 1: The four phases of the study. The psychological constructs examined in the experiment are italicized.

#### 3.2.3 Study order

Before the start of the experiment, each participant was presented with an informed consent form containing the details of the study, and explaining data handling practices. After the acknowledgement of the consent, participants were redirected to the experiment.

***1. Entry questionnaires.*** First we measured curiosity using a previously validated scale obtained from Kashdan et al. [34] (Appendix A). The scale measures two dimensions of curiosity: *stretching* and *embracing*. Stretching is having the motivation to seek new experiences and knowledge, whilst embracing is the general intention to embrace new, unexpected and unpredictable aspects of everyday life. The construct was measured on a five points Likert scale, and the participants were asked to state to what extent the presented sentences reflected the way they would behave or feel (1 - slightly, 5 - extremely; Appendix A).

Next, we measured affect before displaying privacy notices to ensure that the stimuli elicited its expected affective state. We utilized the validated Affective Self Report (ASR) scale to estimate levels of valence and arousal [31] (Appendix B). We chose this scale, because it is time-efficient to use, and past research shows its performance is comparable with some physiological measures (e.g., thermography and electroencephalography) [31]. ASR consists of 10 semantic-differential items (five for valence and five for arousal), for example, *Unpleasant – Pleasant* (Appendix B).

***2. Interactive task.*** Next, participants were asked to complete an interactive task. We asked them to imagine they were signing-up to use a well-being application (improving mental and physical health) that contained social features. Next, we asked participants to complete a sign-up form requesting their name, username, and password. We did not collect this information; it was only visible to the participants in their browser to increase the ecological validity. In the task instructions, we informed participants that such personal information would not be collected.

After completing the sign-up form, participants were presented with a notification prompting them to review the application's privacy policy. At this point, each participant was randomly assigned to one of the four study conditions, each presenting a different privacy notice design (for details see the Appendix 6).

The designs were as follow: control with positive framing; control with negative framing; no control with positive framing; no control with negative framing (Figure 2). For participants who were provided control, we used toggle like switches which were defaulted to "Enabled". Participants were able to adjust some of the privacy settings using these switches (e.g., decide whether they wanted to share data, connect data with social networks). In the framing conditions we used anthropomorphic images accompanied with text. The Gunning's Fog Index of readability for the text of privacy policy was 10.75 for control absent, and 10.88 for control present groups, indicating that it should be readable by high school sophomores [70].

***3. Measurement of outcome variables.*** We took a second measurement of affect, and asked participants whether their affective state had changed. Particularly, whether they felt more or less positive or negative, using the same ASR instrument.

Next, we wanted to learn how much of the information participants would be willing to disclose. To do this, we built an instrument based on the scale created by Joinson et al. [32]. The questionnaire contained 14 items, and asked participants whether they would share different types of personal information (Appendix C).

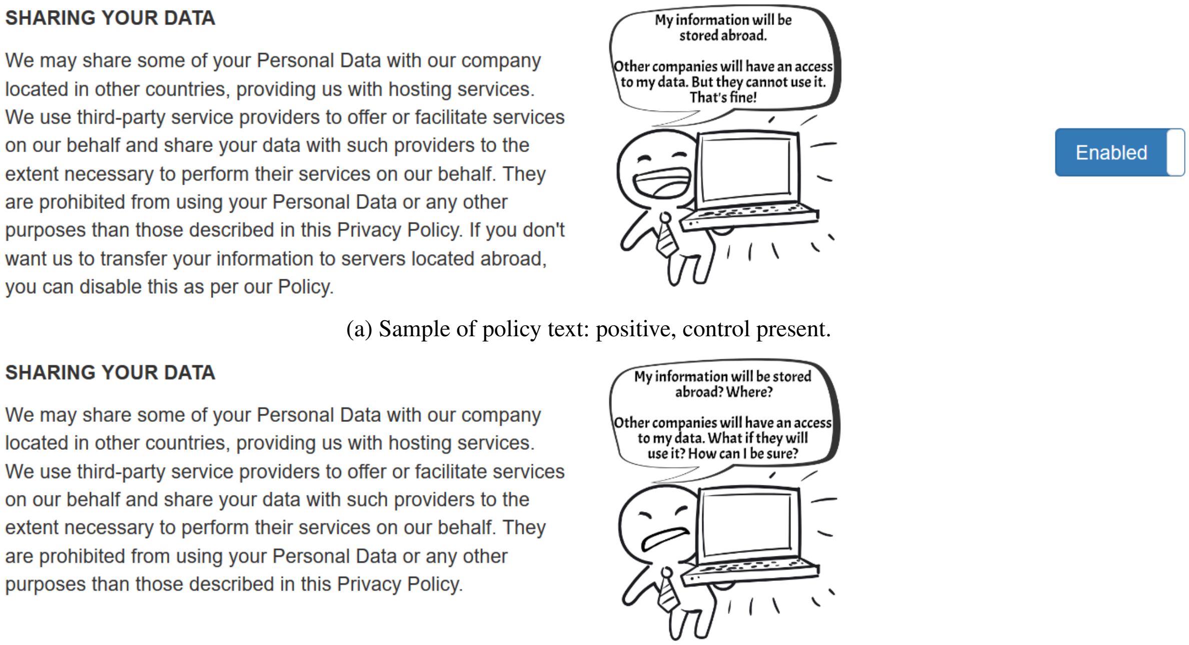
For measuring the participants' comprehension, we created a quiz-like instrument with statements describing information included in the privacy notice (Appendix D). They were presented with ten sentences and asked to declare whether the statement was "True", "False", or "I don't remember / I don't know."

***4. Exit questionnaires.*** We measured privacy-related beliefs, using previously validated instruments. Specifically, we obtained privacy concerns and trust beliefs scales from Malhotra et al. [45] (Appendix F and E).

Last, we asked participants about their demographic characteristics: age, gender, nationality, and education.

## 3.3 Participants

We used an online crowd-sourcing platform, Prolific, to gather participants. The platform enabled us to compensate participants for their work (£9.82/hr). We wanted to gather participants from English speaking countries, and Prolific's participants pool contains mostly respondents from the UK. To participate in the study, each respondent had to read and agree



SHARING YOUR DATA

We may share some of your Personal Data with our company located in other countries, providing us with hosting services. We use third-party service providers to offer or facilitate services on our behalf and share your data with such providers to the extent necessary to perform their services on our behalf. They are prohibited from using your Personal Data or any other purposes than those described in this Privacy Policy. If you don't want us to transfer your information to servers located abroad, you can disable this as per our Policy.

My information will be stored abroad.
Other companies will have an access to my data. But they cannot use it. That's fine!
Enabled

(a) Sample of policy text: positive, control present.

SHARING YOUR DATA

We may share some of your Personal Data with our company located in other countries, providing us with hosting services. We use third-party service providers to offer or facilitate services on our behalf and share your data with such providers to the extent necessary to perform their services on our behalf. They are prohibited from using your Personal Data or any other purposes than those described in this Privacy Policy.

My information will be stored abroad? Where?
Other companies will have an access to my data. What if they will use it? How can I be sure?

(b) Sample of policy text: negative, control absent.

Figure 2: Excerpts of privacy notifications. The notifications' texts were identical between groups, with an exception in the group provided with control (instructional text and the last sentence in the paragraph containing the toggles; Appendix G). The facial expressions of anthropomorphic figures and the accompanying texts were used to elicit positive and negative framing (Appendix G.2).

with the informed consent. Only participants 18 years old or more were allowed to participate in the study.

In total, we received 650 responses. After cleaning the data and removing univariate and multivariate outliers (Mahalanobis distance), the final data-set included 620 cases. The participants were predominantly female (59%); mostly from the UK (74.2%). The respondents were mostly educated (36.1% with Bachelor's degree) and predominantly young (39.5% between 25–34 years old). The detailed demographic characteristics are presented in Table 2.

## 4 Results

In this section, we first discuss the validity and reliability of instruments applied in the current work. Next, we present the main results concerning the research questions.

### 4.1 Validity and reliability of scales

To increase the validity and reliability of our study, when possible, we utilized validated instruments acquired from past research. We checked reliability with statistical tests (factor analysis and scales' reliability estimated with Cronbach's $\alpha$ measurements of internal consistency).

***Intention to disclose.*** We asked participants to what extent they would be willing to disclose different types of information. In total, there were 14 types of information, e.g., name, health-related data, or personal economic situation (Appendix C). To score, participants could choose one of two options: "I would disclose" (1) or "I would prefer not to say" (0). Internal consistency of the scale was acceptable ($\alpha = 0.90$). To compute the variable, we summed the scores.

***Privacy comprehension.*** Privacy comprehension was measured as the awareness of information displayed in the privacy notice. The scale consisted of 10 statements associated with the information included in the privacy policy, focusing on information highlighted in framing messages (Appendix D). Participants were asked to state whether each statement was "True", "False", or select "I do not remember / I do not know". Correct answers scored 1, while incorrect, and cases where participants selected the latter option, scored 0. The latter option was presented to the participants to reduce the potential effects of guessing. Because the instrument aimed to measure knowledge, not a latent construct, we could not check Cronbach's reliability. The variable was computed as the sum of correct answers.

***Privacy concerns and trust.*** Both traits were assessed with instruments obtained from Malhotra et al. [45]. The trust beliefs scale contained five items that aimed to measure general attitude towards online companies (Appendix E). Similarly,

Table 2: Detailed demographic characteristics of the sample.

| Demographic | | N | % |
|---|---|---|---|
| *Gender* | Female | 366 | 59 |
| | Male | 243 | 39.3 |
| | Other/Self identify | 4 | 0.6 |
| | Prefer not to say | 7 | 1.1 |
| *Age* | 18-24 | 103 | 16.6 |
| | 25-34 | 245 | 39.5 |
| | 35-44 | 135 | 21.8 |
| | 45-54 | 74 | 11.9 |
| | 55+ | 63 | 10.2 |
| *Nationality* | UK | 460 | 74.2 |
| | USA | 139 | 22.4 |
| | Ireland | 11 | 1.8 |
| | Other | 10 | 1.6 |
| *Education* | No school/School, no diploma | 21 | 3.4 |
| | High school | 101 | 16.3 |
| | College credit, no degree | 92 | 14.8 |
| | Professional/associate degree | 76 | 12.3 |
| | Bachelor's degree | 224 | 36.1 |
| | Master's degree | 96 | 15.5 |
| | Doctorate degree | 10 | 1.6 |

the privacy concerns scale measured the general approach to online privacy (Appendix F). The two instruments contained seven-point scoring answers, anchored from "Strongly disagree" to "Strongly agree". Both scales underwent the same procedures during which we ran principal component analysis (PCA), and checked Cronbach's reliability. Privacy concerns did not load strongly into one factor, and after revision, two items were deleted. Both scales had good internal consistency, privacy concerns $\alpha = 0.82$, and trust $\alpha = 0.91$.

***Affective state.*** We measured affective state with ASR to distinguish two dimensions: valence and arousal [31] (Appendix B). To confirm whether the instrument measurements were correct, we first ran PCA. In the case of both pre-, and post-stimulus data, the PCA did not load correctly. The valence loaded strongly into one factor, and its reliability scores were acceptable. Both pre-, and post-stimulus scores of internal consistency were acceptable, $\alpha = 0.91$. We created a pre-, and post-stimulus valence variables by computing the mean score for each scale. These new variables were employed in further analysis. The inappropriate loadings of the items measuring arousal undermined the scale's validity and reliability. Hence, we excluded the arousal scale from further analysis.

***Personality characteristic: curiosity.*** Few curiosity related constructs might be measured. One of them is the Need for Cognition (NFC) — "a dispositional variable reflecting the tendency toward thoughtful analysis and reflective thinking" [62]. In our work, we did not use NFC as it relates to complex, effortful decisions [15, 33], while our research was focused on Type 1 processing. We measured a related, but broader construct of curiosity with an instrument comprising of ten items, acquired from Kashdan et al. [34] (Appendix A). The original scale intended to measure two dimensions of curiosity: *stretching* and *embracing*. We ran PCA to confirm whether the items load correctly. Unfortunately, they did not. Instead, the *stretching* facet loaded strongly to one dimension, while *embracing* loaded to both. Both scales had good internal consistency (*stretching* $\alpha = 0.81$; *embracing* $\alpha = 0.84$). Because of unreliable loadings, in further analysis, we used only the curiosity stretching dimension. We used means to compute the curiosity variable. To apply it as an independent variable, based on the median value, we divided curiosity into a two-level categorical variable (low vs high).

## 4.2 Main results

Our data analysis is structured around the outcome variables. Hence, first, we present tests' assumptions and correlations to explain our statistical choices. Next, we present models explaining privacy comprehension (**RQ3**, **RQ4**), intention to disclose (**RQ1**, **RQ5**), and the role of affect (**RQ2**).

We checked parametric assumptions which were good, with slight violations of normality, acceptable in large samples. To establish whether the variables included in the experiment are related, we ran the Pearson correlation analysis. We considered an additional variable in the correlation analysis: time spent on the page displaying privacy notice. The test results revealed mostly small to moderate correlations between some of the variables. Table 3 presents the correlations' details.

In order to check changes in valence, we compared pre-, and post-stimulus scores. We used pairwise t-test to investigate changes. There was a significant difference in the scores for pre-stimulus ($M = 3.63$, $SD = 0.85$) and post-stimulus ($M = 2.71$, $SD = 0.65$) valence; $t(619) = 22.62$, $p < 0.001$, $d = 0.91$. Therefore, we presumed that either framing or control had influenced shifts in valence.

To investigate the research questions, we applied different statistical methods: univariate and multivariate analyses of covariance. We checked tests' assumptions, such as univariate and multivariate normality, outliers (Mahalanobis distance), linearity, absence of multicollinearity (correlation tests), homogeneity (Box's M and Levene's tests), homoscedasticity (scatterplots).

In further analysis, we compared between- and within-group effects based on the independent variables. The group sizes differed as presented in Table 4.

### 4.2.1 Effects on comprehension

To select an appropriate test (univariate or multivariate) we examined correlations. Low correlations ($r < 0.20$) imply that variables should be investigated separately, while moderate correlations ($r$ between 0.20 and 0.50) imply that variables should be analyzed together [12] . Correlations between comprehension and disclosure, as well as between comprehension

Table 3: Correlations between variables: curiosity stretch (CUR), valence pre-stimulus (VAL_PR), valence post-stimulus (VAL_PO), privacy comprehension (COMP), intention to disclose (DIS), privacy concerns (PCS), trust and time spent on policy page. ** significant at 0.01 level; * significant at 0.05 level.

| | CUR | VAL_PR | VAL_PO | COMP | DIS | PCS | TRUST | TIME |
|---|---|---|---|---|---|---|---|---|
| CUR | 1 | 0.23** | 0.04 | 0.09* | 0.08* | 0.08* | 0.00 | -0.00 |
| VAL_PR | | 1 | 0.16** | 0.10* | 0.07 | 0.11** | 0.13** | 0.10** |
| VAL_PO | | | 1 | -0.14** | 0.24** | -0.06 | 0.31** | -0.17** |
| COMP | | | | 1 | -0.08* | -0.05 | -0.03 | 0.50** |
| DISC | | | | | 1 | -0.25** | 0.30** | -0.14** |
| PCS | | | | | | 1 | -0.19** | 0.19 |
| TRUST | | | | | | | 1 | -0.11** |

Table 4: Number of participants per independent variables.

| | Presence of control | | Framing | | Curiosity | | Control over information | |
|---|---|---|---|---|---|---|---|---|
| | Present | Absent | Positive | Negative | Low | High | Adjusted | Not adjusted |
| Frequency | 318 | 302 | 310 | 310 | 317 | 303 | 190 | 128 |
| Percent | 51.3 | 48.7 | 50 | 50 | 51.1 | 48.9 | 59.7 | 40.3 |
| Total | 620 | | 620 | | 620 | | 318 | |

and post-stimulus valence were small (Table 3). Hence, to study comprehension, we used univariate analysis of covariance (**RQ3**, **RQ4**).

The Levene's test was good, $p > 0.05$. The model included three independent variables: framing, control, and curiosity; and four covariates: time spent on the policy page, post-stimulus valence, privacy concerns, and trust. We found a significant small between-subject effect of curiosity on comprehension, $F(1,608) = 8.47, p = 0.004, \eta p^2 = 0.01$. The results show that comprehension was significantly higher among the participants with high curiosity ($M = 5.82, SD = 0.10$) than among the participants with low curiosity ($M = 5.37, SD = 0.10$). Further, the time spent on the page with privacy policy had a significant effect on comprehension ($p < 0.001, \eta p^2 = 0.25$).

To further investigate the effects of control on comprehension, we repeated the univariate test only on the data from the participants who were provided with control. For this purpose, we have created a new categorical variable, splitting participants into two groups: the participants that adjusted settings, and the participants that did not adjust them. As a result, the total sample size decreased to 318 participants.

We ran the test with the same parameters. There were significant small effects of curiosity, $F(1,306) = 7.87, p = 0.005, \eta p^2 = 0.02$, and of control, $F(1,306) = 11.11, p = 0.001, \eta p^2 = 0.03$, on comprehension. Again, the participants scoring high on curiosity scored significantly higher on comprehension ($M = 5.79, SD = 0.15$) than those with lower curiosity ($M = 5.21, SD = 0.14$). Similarly, comprehension was significantly higher among the respondents that changed their settings ($M = 5.90, SD = 0.14$) than among the participants who did not use controls ($M = 5.10, SD = 0.17$). Additionally, two covariates had a significant effects on comprehension: time spent on the policy page ($p < 0.001, \eta p^2 = 0.19$) and privacy concerns ($p < 0.05, \eta p^2 = 0.01$).

### 4.2.2 Effects on affect and intention to disclose

To investigate affect (valence) and intention to disclose (**RQ1**, **RQ5**), we ran a multivariate analysis of covariance. The independent variables were framing, control, and curiosity; covariates were pre-stimulus valence, time spent on the policy page, privacy concerns, and trust. The Box's test was good, significant, but at the level $p > 0.01$, which is acceptable for larger samples. The Levene's test for both outcome variables was good, $p > 0.05$.

There was a small but significant main effect of control on combined dependent variables, $F(2,607) = 2.89, p = 0.05, \eta p^2 = 0.009$, Wilks' $\lambda = 0.99$. The between-subject test confirmed that post-stimulus valence significantly differed among the control groups, $F(1,608) = 5.78, p = 0.01, \eta p^2 = 0.009$. Valence scores were significantly higher for the participants provided with control ($M = 2.78, SD = 0.03$) than for those who did not have a control ($M = 2.65, SD = 0.03$). Further, the model resulted in interaction effect between control and curiosity on the combined dependent variables, $F(2,607) = 3.60, p = 0.02, \eta p^2 = 0.01$, Wilks' $\lambda = 0.98$. The univariate analysis identified the interaction effect for post-stimulus valence, $F(1,608) = 7.19, p = 0.008, \eta p^2 = 0.01$) (Figure 3). The mean scores for valence were higher among the participants provided with control who scored higher on curiosity ($M = 2.84$) than among the participants who scored lower on curiosity ($M = 2.72$). However, the participants with high curiosity not given control scored

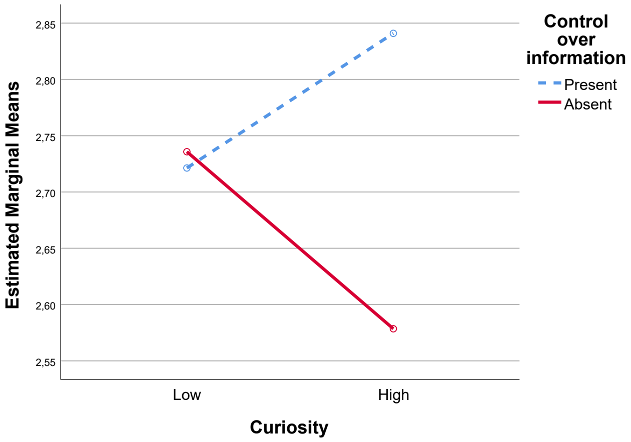


Figure 3: Interaction effect on post-stimulus valence. Covariates appearing in the model are evaluated at the following values: pre-stimulus valence= 3.63, time on policy page= 84.55, privacy concerns= 4.78, trust= 3.10.

lower in valence ($M = 2.73$) than those with lower curiosity ($M = 2.57$).

The covariates had significant effects, $p < 0.001$. Particularly, time spent on the policy page and trust affected outcome variables; pre-stimulus valence influenced post-stimulus valence; privacy concerns significantly affected intention to disclose.

Consistent with the tests of comprehension, we re-ran the analysis on the smaller sample, considering only participants provided with control. Both Box's and Levene's tests were insignificant, $p > 0.05$.

The multivariate test results indicated small significant effect of curiosity, $F(2,305) = 2.99, p = 0.05, \eta p^2 = 0.01$, Wilks' $\lambda = 0.98$. However, the univariate tests results did not confirm it. Further, the multivariate test revealed a small effect of adjusted settings, $F(2,305) = 7.55, p = 0.001, \eta p^2 = 0.04$, Wilks' $\lambda = 0.95$. The univariate test confirmed that the groups differed in intention to disclose, $F(1,306) = 12.68, p < 0.001, \eta p^2 = 0.04$, which was significantly higher among the participants who did not adjust settings ($M = 9.66, SD = 0.37$), than among those who adjusted them ($M = 7.84, SD = 0.29$).

### 4.2.3 The role of affect

The above statistical models revealed that the stable factors influenced intention to disclose. Following the conceptual framework proposed by Dinev et al. [13], and the current results, we sought to investigate further the relationship between these factors and behavioral outcomes (**RQ2**).

First, we ran bootstrapped mediation analysis [27] to identify whether privacy concerns mediated the influence of trust on the intention to disclose.

Table 5: Results of mediation analysis: trust→privacy concerns→intention to disclose.

| Predictor | Coeff. | *SE* | *t* | *p* |
|---|---|---|---|---|
| | *Privacy concerns* | | | |
| *TRUST* | -0.17 | 0.03 | -5.03 | <0.001 |
| | $R^2 = 0.04$ | | | |
| | $F(1,618) = 25.36, p < 0.001$ | | | |
| | *Intention to disclose* | | | |
| *TRUST* | 0.85 | 0.12 | 7.03 | <0.001 |
| *PRIVACY CONCERNS* | -0.70 | 0.13 | -5.20 | <0.001 |
| | $R^2 = 0.09$ | | | |
| | $F(1,617) = 47.42, p < 0.001$ | | | |
| | Intention to disclose (total effect) | | | |
| *TRUST* | 0.977 | 0.12 | 8.06 | <0.001 |
| | $R^2 = 0.09$ | | | |
| | $F(1,618) = 65.05, p < 0.001$ | | | |

The results of simple mediation, demonstrated that trust indirectly influenced the intention to disclose through its effect on privacy concerns. The analysis showed that trust was a significant predictor of privacy concerns, $b = -0.17, t(618) = -5.03, p < 0.001$. Privacy concerns were significantly predicting intention to disclose, $b = -0.70, t(617) = -5.12, p < 0.001$. There was a significant effect of trust predicting disclosure, mediated by privacy concerns, $b = 0.97, t(618) = 8.06, p < 0.001$. Lastly, the direct effect of trust on intention to disclose was also significant, $b = 0.85, t(618) = 7.03, p < 0.001$. The analysis of direct and indirect effects showed that the indirect effect $= 0.12, SE = 0.03$ was significant with bias-corrected bootstrap CI 95%$[0.06, 0.20]$. Thus, the presence of mediation was confirmed.

After establishing the mediation effect, we wanted to examine the role of valence. We used the index of moderated mediation to evaluate whether moderated mediation was present. When bootstrapped confidence intervals of the index of moderated mediation do not include zero, it is assumed that the relationship between the indirect effect and the moderator is not zero, indicating presence of moderated mediation [28]. Additionally, an index not including zero indicates that "any two indirect effects conditioned on different values of [moderator] are statistically different from each other" [28, p. 14]. Hence, there is no need to probe the moderator via further statistical tests.

We examined whether a different level of valence influenced the indirect relationship between trust and intention to disclose. We looked for an interaction effect, either at the first or the second stage of the path model. Figure 4 shows paths in the model, and Table 6 presents the model's results.

There was an interaction effect (Figure 5) at the first stage

Table 6: Moderated mediation: trust→privacy concerns→intention to disclose; moderator: valence.

| | | Consequent | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | M (Privacy Concerns) | | | | Y (Intention to disclose) | | |
| Antecedent | | Coeff. | *SE* | *p* | | Coeff. | *SE* | *p* |
| X (Trust) | $a_1$ | -0.63 | 0.13 | <0.001 | $c_1'$ | 0.80 | 0.44 | 0.07 |
| M (Privacy concerns) | | | | | $b$ | -0.70 | 0.13 | <0.001 |
| W (Valence) | $a_2$ | -0.52 | 0.15 | <0.001 | $c_2'$ | 1.05 | 0.51 | 0.04 |
| X × W | $a_3$ | 0.16 | 0.04 | <0.001 | $c_3'$ | -0.03 | 0.14 | 0.81 |
| Constant | $i_M$ | 6.76 | 0.42 | <0.001 | $i_Y$ | 6.77 | 1.68 | <0.001 |
| | | $R^2 = 0.06$ | | | | $R^2 = 0.15$ | | |
| | | $F(3,616) = 13.17, p < 0.001$ | | | | $F(4,615) = 28.41, p < 0.001$ | | |

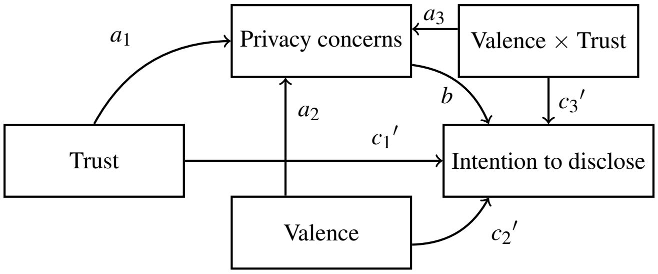


Figure 4: Paths in the model of moderated mediation.

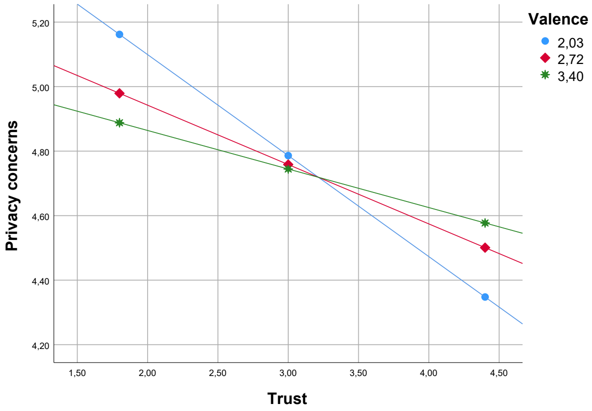


Figure 5: Interaction effect: moderated mediation.

of the model ($a_2$ in Figure 4). The relationship between trust and privacy concerns was moderated by valence. The analysis shows that among the participants with low trust and low valence, scores for privacy concerns were higher than among the participants with low trust and high valence. However, this effect is reversed among the participants with higher trust levels. Among those, the participants with low valence scored lower in privacy concerns than those with a high level of valence.

The bootstrapped index of moderated mediation was significant, confirming that there is an indirect effect of trust on the intention to disclose when controlling for privacy concerns, moderated by valence. The analysis of the conditional effect of focal predictor at values of the moderator showed that at scores of valence smaller than 2.71, trust and privacy concerns were significantly related, $b = -0.19, t(3,616) = -5.26, p < 0.001$, CI 95%$[-0.2, -0.1]$. With the decrease of valence, the relationship between trust and concerns becomes more negative, with the lowest score on valence 2.03, $b = -0.30, t(3,616) = -0.6, p < 0.001$, CI 95%$[-0.4, -0.2]$.

## 5 Discussion

In this section, we discuss our findings according to our two stated contributions. We present both practical implications and research insights for designers and researchers, respectively. Limitations and directions for future work conclude our discussion.

### 5.1 Practical implications

***Affect.*** Our first research question asked *"does visual design of privacy notices influence affective states?"* (**RQ1**). Our findings show that designs providing control combined with curiosity may lead to an increase in valence. People might feel more positive (e.g., happy, pleased, satisfied) when provided with control, but only when holding high levels of curiosity. Our findings suggest that control increased general satisfaction with the design. Such results strengthen our prior exploratory findings [37], which showed that participants expressed a desire for control and choice when consenting to privacy notices.

As aforementioned, increased valence may influence satisfaction, which is one of the key elements contributing to usability (next to efficiency and effectiveness of use) [30]. Considering usability, Habib et al. [25, 26] found that current choices and controls implemented in privacy notices frequently lacked usability as they are inconsistent in their design, and challenging to understand from users perspective. Such designs often require users to go through a lengthy process (e.g., a few clicks, links redirecting users to different pages) before reaching the UI containing privacy controls. This has been further explored by Nouwens et al. [52], who found that participants would consent to a privacy policy without seeking additional controls, if the controls were not placed on the first page of the consent screen. Further, Schaub et al. [57] discussed layered designs of privacy notices (i.e., interactive privacy notice instead of a single block of text), considering them as a way to overcome the status quo of notice and choice. Taking into account past research and our findings, it appears that control given during the sign-up process can carry the potential to increase the usability of privacy-related interactions.

***Comprehension.*** Our fourth research question asked *"does visual design of privacy notices affects comprehension?"* (**RQ4**). The results did not confirm such a relationship, which suggests that differently framed notices have had no influence on privacy comprehension. However, in addressing our third research question, *"does curiosity influence privacy comprehension?"* (**RQ3**), we determined that curiosity positively affected comprehension. Whilst this may sound self-evident, to the best of our knowledge curiosity has not been considered in the design of privacy policies. Oddly, as it is a robust motivational trait that drives human cognitive development [35].

As postulated in the information-gap theory, people seek knowledge to fill the gap in their current understanding [44]. While some people may possess a basic understanding of online privacy, this theory suggests a desire may exist in some users to seek further information. The visual appearance of privacy notices could promote such desires by purposefully designing interfaces that stimulate users' curiosity. For instance, designers could implement methods acquired from game design to encourage user participation and engagement. The intuitive and immediate interactions could be triggered when prompting users to modify settings, instead of idly reading the text of privacy notice. Moreover, privacy designers could follow some of the guidelines for UIs enhancing curiosity, such as those proposed by Malone [46]. Malone postulated evoking curiosity through the *optimal level of informational complexity* — through environments that are "neither too complicated nor too simple with respect to the user's existing knowledge" [46, p. 67]. The optimal level might be achieved with the application of *novelty* and *surprise*, *randomness* and *humor* that could elicit positive experiences, increasing satisfaction. However, such methods would have to be thoroughly tested, as they may bring an inverse effect, and result in dissatisfaction or incomprehensibility.

Perhaps privacy policies arranged into "gradually discoverable" elements of information may be able to activate curiosity and enhance engagement. Such an approach was previously investigated in the context of crowd workers' performance, where it was found to be successful [41]. The progressive revelation of the information improved noticeability, and kept people curious to unravel more information to fill gaps in their knowledge. However, while in the context of privacy such an approach might influence engagement and prominence of information, applied to real-life situations, it could result in habituation effects or be disruptive during the application sign-up process. Taking into consideration previous findings, and recognizing the small effect sizes of our results, we believe that "gradually discoverable" privacy notices need to be thoroughly researched to establish their efficacy and efficiency during an application sign-up.

***Control.*** In our fifth research question, we asked, *"does visual design of privacy notices affect intention to disclose information?"* (**RQ5**). Our results indicate that among people provided with a choice to adjust their settings, those holding higher levels of curiosity disclosed less information. This finding suggest the need to design privacy notices that provide users with options to set individual preferences, which allow them to adjust the amount and type of information disclosed or shared.

Consistent with our findings, past research found that control influences the value that people attach to personal information, and impacts disclosure [1]. Hence, our results supported by prior findings, indicate that future designs of privacy notices affording people with greater levels of usable control may be able to improve information disclosures. Still, we recognize that such solutions might be untimely and difficult to implement, as they require severe modifications in the system design or business models. Further, such solutions might restrict access to the complete functionality of an application, leading to the potential loss of a customer or disparity in service levels between users.

On the other hand, providing users with control may have a positive effect on companies. Improved usability may encourage users to utilize an application, perceiving it as more attractive due to enhanced transparency around information disclosures. Additionally, providing control may increase legal compliance, e.g., the fulfillment of the GDPR's requirements.

***Importance of time.*** We found that the time spent on the notice page had a significant influence on comprehension, having an effect size larger than other variables. This finding indicates that people contributing their time to gather information are more aware of the privacy notice. We interpret this result as a call for designs of notices that engage users to spend more time on the notice's page. Perhaps the methods discussed above, such as the incremental revelation of information or layered designs of privacy notices might have such an effect.

***Concerns, trust, and valence.*** Our findings suggest that valence moderates the relationship between trust and privacy concerns. Such a result might be applied to privacy UI designs with malicious intentions in mind. For instance, as the *dark pattern* that might influence valence, and lead to manipulating users' attitude towards lesser concerns. Effectively, this might "trick" users into disclosing more. On the other hand, we believe that such a result could be implemented in UI to increase privacy concerns. For example, by highlighting risks and harms to privacy through interface design, which may lower valence, and result in a more negative relationship between trust and concerns, indirectly reducing information disclosure.

### 5.2 Research insights

***Concerns, trust, and valence.*** Our second research question asked, *"what is the role of the affective state in the relationship between attitudinal factors and intention to disclose?"* (**RQ2**). According to our findings, privacy concerns mediate the relationship between trust and disclosure. More importantly, our results show that valence is moderating such a relationship. It seems that lower trust leads to greater privacy concerns; however, the affective state may alter the direction of this relationship. Our findings suggest that an increase in valence diminishes the effects of trust on concerns, which might be interpreted as the possibility to alter privacy concerns via elicitation of different emotional states.

To the best of our knowledge, little attention has been given to the role of affect in privacy-related decision making. Our results call for future privacy studies, which address this gap, focusing on the role of affective states in different contexts. Studying affect may contribute to a greater understanding of cognitive processes active during day-to-day privacy-related actions, and consequently may have practical implications.

Additionally, our findings confront the *privacy paradox*, and demonstrate a significant relationship between trust, privacy concerns, and intention to disclose. Perhaps, the phenomenon is not present in the context of a well-being application sign-up process, in which people's behaviors are aligned with their beliefs.

***Cognitive processing.*** The moderating effect of valence suggests that intention to disclose might be an effect of the Type 1 processing, which utilizes mental shortcuts and simple solutions as the means for information processing. Further, our results indicate that the affect-as-information and feeling-as-information theories may be applied in the privacy research [9,58]. Our findings demonstrate that concerns increase with a decrease in valence. Perhaps because of the negative valence, people perceive the situation as unsafe, using affect as an indicator / marker of safety.

### 5.3 Limitations and future work

We used a crowdsourcing platform and gathered participants mostly from English speaking countries, which make our findings less generalizable to a wider population. We examined only one context of privacy interaction, a sign-up process for the well-being application. Recognizing the contextuality of privacy, the sign-up process for another type of application could lead to different conclusions.

Additionally, we might have primed participants by exposing them to privacy controls, and as a result, affect their intention to disclose. However, if this was the case, we might perceive such priming as a relevant outcome, demonstrating that solely the presence of controls has the potential to make people more privacy-conscious.

Our statistical analysis resulted in small effect sizes, which is anticipated in exploratory studies. However, our results are significant, and the effects found provide motivation for future replication studies to determine the magnitude of our findings. Additionally, it is essential to mention that the interpretation of the effect sizes for models with covariates is challenging, as they are difficult to compare to standard benchmarks defined by Cohen, which were based on unrestricted populations [40]. Cohen was cautiously discussing these benchmarks, acknowledging that they might not apply to all research areas [56]. More recent findings revealed that he might have been correct, as there are significant differences in effect sizes between different sub-disciplines of psychology, with the actual effect sizes being lower than the commonly used criteria [56].

Considering the limitations mentioned above, we propose that future work should include comparable experiments, but place them in diverse settings, targeting different population and privacy contexts. Further, we call for research incorporating methods different than self-reported measures, particularly in the case of affect. Both observational data, as well as physiological measurements (e.g., EEG, fMRI), could be applied in future inquiries to assess levels of affect more accurately.

## 6 Conclusion

We conducted an empirical analysis of privacy interactions during the application sign-up process. To gather the necessary data, we ran an online experiment with 620 English speaking participants. Our results show that people driven by curiosity utilize control over their information. We examined how this affects their intention to disclose, privacy comprehension, and affective state (positive–negative valence). Further, we investigated the role of valence in the relationship between trust and privacy concerns. Our research indicates that the visual design of privacy notices may have a beneficial influence on personal information disclosures. However, other factors should be taken into consideration to ensure improvement in individuals' privacy practices. We discuss our findings in the context of their applicability to the design of privacy notices as well as future research directions, calling for a change in both practical and theoretical approach to privacy research.

## Acknowledgment

This work has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730 (Privacy&Us Innovative Training Programme).

## References

[1] A. Acquisti, M. Sleeper, Y. Wang, S. Wilson, I. Adjerid, R. Balebako, L. F. Brandimarte, L.and Cranor, S. Komanduri, P. G. Leon, N. Sadeh, and F. Schaub. Nudges for Privacy and Security. *ACM Computing Surveys*, 50(3):1–41, 2017.

[2] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein. Sleights of Privacy : Framing , Disclosures , and the Limits of Transparency. *Symposium on Usable Privacy and Security (SOUPS)*, page 17, 2013.

[3] J. Angulo, S. Fischer-Hübner, E. Wästlund, and T. Pulls. Towards usable privacy policy display and management. *Information Management & Computer Security*, 20(1):4–17, 2012.

[4] G. Bente, T. Dratsch, S. Rehbach, M. Reyl, and B. Lushaj. Do you trust my avatar? Effects of photo-realistic seller avatars and reputation scores on trust in online transactions. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8527 LNCS:461–470, 2014.

[5] L. Brandimarte, A. Acquisti, and G. Loewenstein. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, 4(3):340–347, 2013.

[6] B. Brown. Studying the Internet experience. *HP Laboratories Technical Report HPL*, 2001.

[7] California State Legislature. SB-1121 California Consumer Privacy Act of 2018, 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[8] E. K. Choe, J. Jung, B. Lee, and K. Fisher. Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing. In *IFIP Conference on Human-Computer Interaction*, pages 74–91. Springer, 2013.

[9] G. L. Clore, K. Gasper, and E. Garvin. Affect as information. *Handbook of affect and social cognition*, pages 121–144, 2001.

[10] G. Conti and E. Sobiesk. An Honest Man Has Nothing to Fear: User Perceptions on Web-based Information Disclosure. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS)*, page 112, 2007.

[11] K. P. L. Coopamootoo and T. Groß. Why Privacy Is All But Forgotten. *Proceedings on Privacy Enhancing Technologies*, 2017(4):97–118, 2017.

[12] P. Dattalo. *Analysis of multiple dependent variables*. Oxford University Press, 2013.

[13] T. Dinev, A. R. Mcconnell, and H. J. Smith. Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. *Information Systems Research*, 26(4):639–655, 2015.

[14] S. Egelman. My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2369–2378, 2013.

[15] S. Epstein, R. Pacini, V. Denes-Raj, and H. Heier. Individual Differences in Intuitive-Experiential and Analytics-Rational Thinking Styles. *Journal of Personality and Social Psychology*, 71(2):390–405, 1996.

[16] European Commission. EU general data protection regulation (GDPR) 2016/679, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[17] European Commission. Special Eurobarometer 487a: The General Data Protection Regulation. Technical Report March, EC, 2019.

[18] J. B. T. Evans and K. E. Stanovich. Dual-Process Theories of Higher Cognition: Advancing the Debate. *Perspectives on Psychological Science*, 8(3):223–241, 2013.

[19] A. Felt, E. Ha, S. Egelman, and A. Haney. Android permissions: User attention, comprehension, and behavior. In *Symposium on Usable Privacy and Security*, SOUPS ’12, pages 1–16, 2012.

[20] M. L. Finucane, A. Alhakami, P. Slovic, and S. M. Johnson. The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, 13(1):1, 2000.

[21] N. Gerber, P. Gerber, and M. Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*, 77:226–261, 2018.

[22] A. Ghorayshi and S. Ray. Buzzfeed - grindr is letting other companies see user hiv status and location data, 2018. https://www.buzzfeed.com/azeenghorayshi/grindr-hiv-status-privacy?utm{_}term=.xorXWLx2{#}.mdk3Q5ml.

[23] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal. How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In *Proceedings of the Twelfth*

*USENIX Conference on Usable Privacy and Security*, SOUPS '16, page 321–340, USA, 2016. USENIX Association.

[24] J. Gottlieb, P. Y. Oudeyer, M. Lopes, and A. Baranes. Information-seeking, curiosity, and attention: Computational and neural mechanisms. *Trends in Cognitive Sciences*, 17(11):585–593, 2013.

[25] H. Habib, S. Pearman, J. Wang, Y. Zou, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Conference on Computer Human Interaction (CHI)*, 2020.

[26] H. Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*, pages 387–406, 2019.

[27] A. F. Hayes. Process: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling, 2012.

[28] A. F. Hayes. An Index and Test of Linear Moderated Mediation. *Multivariate Behavioral Research*, 50(1), 2015.

[29] A. Hern. Fitness tracking app Strava gives away location of secret US army bases, 2018. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

[30] International Organization for Standardization. Ergonomics of human-system interaction–part 11: Usability: Definitions and concepts, 2018.

[31] S. Jenkins, R. Brown, and N. Rutterford. Comparing Thermographic, EEG, and Subjective Measures of Affective Experience During Simulated Product Interactions. *International Journal of Design*, 3(2):53–65, 2009.

[32] A. N. Joinson, C. Paine, T. Buchanan, and U. D. Reips. Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior*, 24(5):2158–2171, 2008.

[33] D. Kahneman. A Perspective on Judgment and Choice. *American Psychologist*, 3(4):7–18, 2003.

[34] T. B. Kashdan, M. F. Steger, B. P. Winterstein, W. E. Breen, P. J. Silvia, M. W. Gallagher, and D. Terhar. The curiosity and exploration inventory-II: Development, factor structure, and psychometrics. *Journal of Research in Personality*, 43(6):987–998, 2009.

[35] C. Kidd and B. Y. Hayden. The Psychology and Neuroscience of Curiosity. *Neuron*, 88(3):449–460, 2015.

[36] Y.-S. Kim, K. Reinecke, and J. Hullman. Explaining the gap: Visualizing one's predictions improves recall and comprehension of data. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 1375–1386, 2017.

[37] A. Kitkowska, Y. Shulman, L. A. Martucci, and E. Wästlund. Facilitating privacy attitudes behaviors with affective visual design. In *To appear in: 35th International Conference on ICT Systems Security and Privacy Protection – IFIP SEC 2020*, 2020.

[38] A. Kitkowska, Y. Shulman, L. A. Martucci, and E. Wästlund. Psychological effects and their role in online privacy interactions: A review. *IEEE Access*, 8:21236–21260, 2020.

[39] B. P. Knijnenburg and A. Kobsa. Making Decisions about Privacy: Information Disclosure in Context-Aware Recommender Systems. *ACM Transactions on Interactive Intelligent Systems*, 3(23), 2013.

[40] D. Lakens. Calculating and reporting effect sizes to facilitate cumulative science: A practical primer for t-tests and ANOVAs. *Frontiers in Psychology*, 4(NOV):1–12, 2013.

[41] E. Law, M. Yin, J. Goh, K. Chen, M. A. Terry, and K. Z. Gajos. Curiosity killed the cat, but makes crowdwork better. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 4098–4110, New York, NY, USA, 2016. Association for Computing Machinery.

[42] J. S. Lerner, Y. Li, P. Valdesolo, and K. S. Kassam. Emotion and decision making. *Annual Review of Psychology*, 66:799–823, 2015.

[43] H. Li, R. Sarathy, and H. Xu. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, 51(3):434–445, 2011.

[44] G. Loewenstein. The Psychology of Curiosity: A Review and Reinterpretation. *Psychological Bulletin*, 116(1), 1994.

[45] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[46] T. W. Malone. Heuristics for designing enjoyable user interfaces: Lessons from computer games. In *Proceedings of the 1982 Conference on Human Factors in Computing Systems*, CHI '82, page 63–68, New York, NY, USA, 1982. Association for Computing Machinery.

[47] T. Mirsch, C. Lehrer, and R. Jung. Digital Nudging: Altering User Behavior in Digital Environments. *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, pages 634–648, 2017.

[48] S. Monteleone, R. Van Bavel, N. Rodríguez-Priego, and G. Esposito. Nudges to privacy behaviour: Exploring an alternative approach to privacy notices. *JRC Science and Policy Report. Luxembourg, Luxembourg: Publications Office of the European Union*, 2015.

[49] H. Nissenbaum. A contextual approach to privacy online. *Daedalus*, 140(4):32–48, 2011.

[50] E. Noll Webb, G. Balasubramanian, U. OBroin, and J. M. Webb. WHAM! POW! Comics as User Assistance. *Journal of Usability Studies*, 7(3):105–117, 2012.

[51] P. A. Norberg, D. R. Horne, and D. A Horne. The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, 41(1):100–126, 2007.

[52] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Conference on Human Factors in Computing Systems(CHI)*, 2020.

[53] C. Phelan, C. Lampe, and P. Resnick. It's Creepy, But It Doesn't Bother Me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5240–5251, San Jose, 2016.

[54] P. Rajivan and J. Camp. Influence of privacy attitude and privacy cue framing on android app choices. In *Twelfth Symposium on Usable Privacy and Security*, 2016.

[55] J. A. Russell and L. F. Barrett. Core Affect, Prototypical Emotional Episodes, and Other Things Called Emotion: Dissecting the Elephant. *Journal of Personality and Social Psychology*, 76(5), 1999.

[56] T. Schäfer and M. A. Schwarz. The meaningfulness of effect sizes in psychological research: Differences between sub-disciplines and the impact of potential biases. *Frontiers in Psychology*, 10(APR):1–13, 2019.

[57] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A Design Space for Effective Privacy Notices. In *Symposium on Usable Privacy and Security (SOUPS) 2015*, pages 1–17, Ottawa, Canada, 2015.

[58] N. Schwarz. Feelings-as-Information Theory. *Handbook of Theories of Social Psychology: Volume 1*, pages 289–308, January 2012.

[59] F. Slovic. The Affect Heuristic. In *Heuristics and Biases; The Psychology of Intuitive Judgement*, pages 397–420. Cambridge University Press, 2002.

[60] J. H. Smith, T. Dinev, and H. Xu. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(December):989–1015, 2011.

[61] D. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):477–560, 2006.

[62] K. E. Stanovich and R. F. West. Individual differences in reasoning: implications for the rationality debate? *The Behavioral and brain sciences*, 23(5):645–665; discussion 665–726, 2000.

[63] A. Sutcliffe and A. Namoune. Getting the Message across: Visual Attention, Aesthetic Design and What Users Remember. In *Proceedings of the 7th ACM Conference on Designing Interactive Systems*, DIS '08, page 11–20, New York, NY, USA, 2008. Association for Computing Machinery.

[64] M. Tabassum, A. Alqhatani, M. Aldossari, and H. Richter Lipford. Increasing User Attention with a Comic-Based Policy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, New York, NY, USA, 2018. Association for Computing Machinery.

[65] M. Taddicken. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, 19(2):248–273, 2014.

[66] D. Tasse, A. Ankolekar, and J. Hailpern. Getting Users' Attention in Web Apps in Likable, Minimally Annoying Ways. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, pages 3324–3334, 2016.

[67] A. Toet, D. Kaneko, S. Ushiama, S.e Hoving, I. de Kruijf, A. M. Brouwer, V. Kallen, and J. B.F. van Erp. EmojiGrid: A 2D Pictorial Scale for the Assessment of Food Elicited Emotions. *Frontiers in Psychology*, 9(NOV):1–21, 2018.

[68] T. F. Waddell, J. R. Auriemma, and S. S. Sundar. Make it Simple, or Force Users to Read? Paraphrased Design Improves Comprehension of End User License Agreements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5252–5256, 2016.

[69] N. Wang, B. Zhang, B. Liu, and H. Jin. Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. In *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services*, pages 373–382, 2015.

[70] M. Zamanian and P. Heydari. Readability of Texts: State of the Art. *Theory & Practice in Language Studies*, 2(1), 2012.

[71] B. Zhang, M. Wu, H. Kang, E. Go, and S. S. Sundar. Effects of security warnings and instant gratification cues on attitudes toward mobile websites. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, pages 111–114, 2014.

# Appendix

## A Curiosity

*Participant instructions:*

Rate the statements below for how accurately they reflect the way you generally feel and behave. Do not rate what you think you should do, or wish you do, or things you no longer do. Please be as honest as possible.

1. I actively seek as much information as I can in new situations.
2. I am the type of person who really enjoys the uncertainty of everyday life.
3. I am at my best when doing something that is complex or challenging.
4. Everywhere I go, I am out looking for new things or experiences.
5. I view challenging situations as an opportunity to grow and learn.
6. I like to do things that are a little frightening.
7. I am always looking for experiences that challenge how I think about myself and the world.
8. I prefer jobs that are excitingly unpredictable.
9. I frequently seek out opportunities to challenge myself and grow as a person.
10. I am the kind of person who embraces unfamiliar people, events, and places.

*Scoring:*

Items 1, 3, 5, 7, and 9 reflect curiosity *stretching*. Items 2, 4, 6, 8, and 10 reflect curiosity *embracing*. Items were anchored on the scale: 1 – very slightly or not at all, 2 – a little, 3 – moderately, 4 – quite a bit, 5 – extremely.

## B Affective Self Report

*Participant instructions:*

*1st measurement instructions:* Thinking about yourself, to what extent do you currently feel:

*2nd measurement instructions:* Earlier in the study, we asked you how did you feel. Thinking back about the sign-up process, would you say that now you feel different or the same in comparison to when we previously asked you?

1. Annoyed – Pleased
2. Tired – Energetic
3. Unpleasant – Pleasant
4. Patient – Anxious
5. Irritated – Content
6. Unhappy – Happy
7. Calm – Restless
8. Disappointed – Satisfied
9. Relaxed – Tense
10. Indifferent – Curious

*Scoring:*

Items scored on 7 points Likert scale. The second measurement was labelled with the word *more*, e.g., More Annoyed – More Pleased.

## C Intention to disclose information

*Participant instructions:*

Thinking back about the sign-up process and considering the previously presented scenario, if you were to sign up for this application, would you be willing to share any of the following information with this application provider?

1. Your age
2. Your weight
3. Your height
4. Gender
5. Ethnicity
6. Your sexual orientation
7. Your marital status
8. Number of children
9. Chronic conditions
10. Overall number of sexual partners, since you became sexually active
11. Religious beliefs
12. Employment status
13. Political beliefs
14. Monthly income

*Answers:*

"I would disclose" or "I would prefer not to say."

## D Privacy comprehension

*Participant instructions:*

Thinking back about the sign-up process, could you please tell us which of the following statements you believe are true considering the privacy policy that you have been asked to read.

1. Personal information is any information about you that is collected by an online service provider.

2. Information about you collected through any forms, including sign-up form is used to personalize services.
3. The service provider will collect your health information.
4. You are contractually obliged to provide your contact information.
5. You have full control over your personal information if you sign up for forums and create a public profile on this application, and you control how this information is being shared with others.
6. There are third parties that collect data about you and this service's policy applies to the processing of your information by such third parties.
7. If you are logged in to your social media and use the application at the same time, information about your activities will be tracked and recorded by social media providers.
8. This application transfers personal data to companies located abroad. These services can freely process your personal information for their purposes.
9. The service provider is legally obliged to share your personal information, and it does not need to inform you about it.
10. The service provider can process your personal data without your consent, for any purpose that was not explained in its privacy policy.

*Answers:*

"True", "False", "I don't remember / I don't know."

## E Trust

*Participant instructions:*

Please read the statements below and indicate to what extent you disagree or agree with each of the statements.

1. Online companies would be trustworthy in handling the information.
2. Online companies would tell the truth and fulfil promises related to the information provided by me.
3. I trust that online companies would keep my best interests in mind when dealing with the information.
4. Online companies are in general predictable and consistent regarding the usage of the information.
5. Online companies are always honest with customers when it comes to using the information that I would provide.

*Scoring:*

Items scoring on 7 points Likert scale, anchored "Strongly disagree" – "Strongly agree".

## F Privacy concerns

*Participant instructions:*

Please state, to what extent do you agree with the following sentences.

1. All things considered, the Internet may cause serious privacy problems.
2. Compared to others, I am more sensitive about the way online companies handle my personal information.
3. To me, it is the most important thing to keep my privacy intact from online companies.
4. I believe other people are too much concerned with online privacy issues.
5. Compared with other subjects on my mind, personal privacy is very important.
6. I am concerned about threats to my personal privacy today.

*Scoring:*

Items scoring on 7 points Likert scale, anchored "Strongly disagree" – "Strongly agree."

## G Text of privacy policies

OUR POLICY
On this page, you can find an overview of our privacy policy. If you think the information here is insufficient, you can check the full text of Privacy Policy.

WHAT DATA WE COLLECT AND USE WHEN YOU VISIT OUR SITE
We collect Non-personal and Personal information when you visit our website. Personal Data is information that identifies you or could be used to identify you, e.g., name, address, email. Some of our services require the processing of your health-related data. We collect information that you provide directly to us when you choose to use our Services. We also collect data that you submit through responses to any forms such as sign up or profile creation forms, questionnaires, etc. We use this data to personalize our services and to optimize your experience.

WHEN WE COLLECT YOUR DATA AND WHY
We collect information, e.g., Personal Data, when you browse our website or use our service. Among the information collected are your IP address, browser type, operating system, error logs, and the like. Such aggregated information does not identify you and is used by us to analyze trends, to administer and monitor our site, its use, and to gather general information about the use of our website.

HOW WE DISCLOSE YOUR DATA
There are a few instances when we are obliged to disclose your information. E.g., to pursue our legitimate interest in applying or enforcing the terms and conditions, or to respond to any claims. We may disclose your data to protect our rights or the rights of a third party; to protect the safety of any person or to prevent any illegal activities. If legally required to do so, we will collect your prior consent before sharing your Personal Data with other companies.

HOW WE USE YOUR DATA

We use your data to send you service announcements and updates regarding our Website. You are contractually required to provide us with such Personal Data as, without it, we will not be able to send you service-related communication.

PROCESSING FOR OTHER PURPOSES

If your Personal Data are processed for purposes not mentioned in this policy, we will provide you with information on that other purposes and any additional relevant information as referred to in this Privacy Policy.

SHARING YOUR DATA

We may share some of your Personal Data with our company located in other countries, providing us with hosting services. We use third-party service providers to offer or facilitate services on our behalf and share your data with such providers to the extent necessary to perform their services on our behalf. They are prohibited from using your Personal Data or any other purposes than those described in this Privacy Policy.

SOCIAL FEATURES

We feature public forums such as message boards, bulletin boards or activities where you and other users can communicate with one another. The Public Profile feature permits you to share information about yourself (including, if you elect, Personal Data) with others. If you use Social Features, we cannot control how other users might use your data. We also cannot prevent you from receiving unwanted messages from others. You are not legally required to provide us with your Personal Data, but without it, we cannot offer you to use our Social Features.

SOCIAL PLUGINS

Our Website contains links to or features from other sites. This Policy does not cover the privacy practices of third-party websites or features. We use social networks plugins of Facebook, Twitter and YouTube. If you visit our Website while signed in to your social media account, results in the transfer of information about you to the social network. Such information can be linked with your social network account. This data transfer is triggered already when you visit our Website, irrespective whether you interact with the plugin. To prevent this, you must log out of your social network account before visiting our Website.

CONTACT

If you have any questions about our Privacy Policy or feel that we are not abiding by the terms of our posted Privacy Policy or the applicable data protection laws, please contact our data protection officer at legal@abc.com.

### G.1 Amended text of policy for groups given control

OPT-OUT FROM INFORMATION PROCESSING

We do not want to collect all of the information about you. However, the more information we have, the more accurate and personalized services we can offer. To ensure your control over the information, we offer you options to opt-out from particular data collection and processing. If you wish to limit the collection of your information, change the switches to Disabled mode.

SHARING YOUR DATA

We may share some of your Personal Data with our company located in other countries, providing us with hosting services. We use third-party service providers to offer or facilitate services on our behalf and share your data with such providers to the extent necessary to perform their services on our behalf. They are prohibited from using your Personal Data or any other purposes than those described in this Privacy Policy. If you don't want us to transfer your information to servers located abroad, you can disable this as per our Policy.

SOCIAL FEATURES

We feature public forums such as message boards, bulletin boards or activities where you and other users can communicate with one another. The Public Profile feature permits you to share information about yourself (including, if you elect, Personal Data) with others. If you use Social Features, we cannot control how other users might use your data. We also cannot prevent you from receiving unwanted messages from others. You are not legally required to provide us with your Personal Data, but without it, we cannot offer you to use our Social Features. If you do not want to have Social Features, you can disable this functionality, and we will not provide you with such services.

SOCIAL PLUGINS

Our Website contains links to or features from other sites. This Policy does not cover the privacy practices of third-party websites or features. We use social networks plugins of Facebook, Twitter and YouTube. If you visit our Website while signed in to your social media account, results in the transfer of information about you to the social network. Such information can be linked with your social network account. This data transfer is triggered already when you visit our Website, irrespective whether you interact with the plugin. To prevent this, you must log out of your social network account before visiting our Website. Alternatively, you can disable the social media plugins as offered in our Policy.

### G.2 Images applied in the policy display

Each section of the text in the privacy policy contained framing image, as presented in figs. 6 to 13 (A.- negative, B.- positive).

My personal information is collected, even my health information. I may be identified! They say it will help to personalize this app... but I'm worried that somebody will access my information.
My personal information is collected, even my health information. I may be identified. But it will help to personalize this app. It is worth it, even if someone could access my information!
A.
B.

Figure 6: Images displayed next to the policy section "WHAT DATA WE COLLECT AND USE WHEN YOU VISIT OUR SITE."

They collect my personal information, like IP, browser type etc. Apparently, to identify trends and patterns in data. I am very concerned!
They collect my personal information, like IP, browser type etc. It's all to identify patterns and trends in data, and improve the application! I don't mind!
A.
B.

Figure 7: Images displayed next to the policy section "WHEN WE COLLECT YOUR DATA AND WHY."

They will disclose my information to protect their company or when they are legally obliged. I don't think I like this approach! At least they will first ask me to consent to such disclosure...
They will disclose my information to protect their rights or when they are legally obliged. I think it is understandable. Additionally, they will first ask me to consent to such disclosure!
A.
B.

Figure 8: Images displayed next to the policy section "HOW WE DISCLOSE YOUR DATA."

I must provide my contact details so they could send me updates. But wont they spam me with adds ?! I am worried...
I should provide my contact details so they could send me updates. It is important to have the latest version, otherwise the app my not work properly!
A.
B.

Figure 9: Images displayed next to the policy section "HOW WE USE YOUR DATA."

If my information will be used for purpose other than they told me, they will contact me.

What if I will not notice their messages?!
If my information would be used for purpose other than they told me, they will contact me.

I think this is very reassuring and fair!
A.
B.

Figure 10: Images displayed next to the policy section “PROCESSING FOR OTHER PURPOSES.”

My information will be stored abroad? Where?

Other companies will have an access to my data. What if they will use it? How can I be sure?
My information will be stored abroad.

Other companies will have an access to my data. But they cannot use it. That's fine!
A.
B.

Figure 11: Images displayed next to the policy section “SHARING YOUR DATA.”

If I decide to use social features I will loose control over my information.

That worries me, I would not like anyone to use my personal information!
If I decide to use social features others may get control over my information.

That's fine, I will make sure to share only information that is not personal!
A.
B.

Figure 12: Images displayed next to the policy section “SOCIAL FEATURES.”

If I visit this site while signed to my social media, my data may be linked.

I don't want social media to see what I am doing on this app!
If I visit this site while signed to my social media, my data may be linked.

That is ok! I want to share my information on social media!
A.
B.

Figure 13: Images displayed next to the policy section “SOCIAL PLUGINS.”