Vanessa Bracamonte*, Sebastian Pape, and Sascha Loebner

"All apps do this": Comparing Privacy Concerns Towards Privacy Tools and Non-Privacy Tools for Social Media Content

Abstract: Users report that they have regretted accidentally sharing personal information on social media. There have been proposals to help protect the privacy of these users, by providing tools which analyze text or images and detect personal information or privacy disclosure with the objective to alert the user of a privacy risk and transform the content. However, these proposals rely on having access to users' data and users have reported that they have privacy concerns about the tools themselves. In this study, we investigate whether these privacy concerns are unique to privacy tools or whether they are comparable to privacy concerns about non-privacy tools that also process personal information. We conduct a user experiment to compare the level of privacy concern towards privacy tools and non-privacy tools for text and image content, qualitatively analyze the reason for those privacy concerns, and evaluate which assurances are perceived to reduce that concern. The results show privacy tools are at a disadvantage: participants have a higher level of privacy concern about being surveilled by the privacy tools, and the same level concern about intrusion and secondary use of their personal information compared to non-privacy tools. In addition, the reasons for these concerns and assurances that are perceived to reduce privacy concern are also similar. We discuss what these results mean for the development of privacy tools that process user content.

Keywords: Privacy-Enhancing Technologies, privacy concerns, social media, user study

DOI 10.56553/popets-2022-0062
Received 2021-11-30; revised 2022-03-15; accepted 2022-03-16.

***Corresponding Author: Vanessa Bracamonte:** KDDI Research, Inc., E-mail: va-bracamonte@kddi-research.jp
Sebastian Pape: Goethe University Frankfurt, E-mail: sebastian.pape@m-chair.de
Sascha Loebner: Goethe University Frankfurt, E-mail: sascha.loebner@m-chair.de

1 Introduction

The pace and amount of information sharing on social media has resulted in users' revealing private information, about themselves or others. Users report that they regret sharing this information [49, 57], and there have been proposals for ways to help users protect their privacy on social media. For text data, there are proposals for scoring the privacy information contained in users' social media posts [56] and classifying these posts by the type of personal information they contain [6, 52, 55] with the objective of alerting the user. There are also proposals for anonymizing the social media posts once personal information has been identified [40]. There are similar proposals for image data, in particular for identifying faces and human subjects in photos and applying different transformations to avoid recognition [26, 31].

These proposals rely on access to users' personal information to provide privacy protection, and so they have an element of risk associated with them. However, only few studies discuss issues of privacy concern and trust about privacy tools themselves [39]. In user perception evaluation studies on privacy enhancing tools such as browser extensions for privacy awareness that detect and block third-party tracking [48] and web browsing privacy protection tools [51], users have indicated that they have privacy concerns about tools that have access to information about which sites they visit. There is some research on the perception of users towards different aspects of privacy enhancing tools [24], but research on privacy tools that process text and image data do not often include evaluation of users' privacy concerns towards the tool itself. Bracamonte et al. [4, 5] report that privacy concerns have a negative effect on intention of using privacy tools that process users' social media posts.

Privacy protection is usually not the primary goal of the users, but only their secondary goal [10]. Transferred to our use case this means that the user's main goal is to post something on social media (either an image or a text or a combination of both). If the privacy-enhancing technology (PET) is integrated into the service (e. g. the

Tor browser [12]), the user's aims become more distinct. Thus, from a scientific perspective, "standalone" PETs which are not integrated into a specific service and can optionally be used for several purposes may give a better view on the users' motivation to use PETs since they allow us to focus on the usefulness and perception of the PET with regard to privacy protection and interference with other goals of the user can be avoided [22]. This dilution of the user's aims is particularly strong for health application where the user sometimes has to chose between a function of the health tool and privacy or when the PET is embedded into the health tool, e. g. as it is done in contact tracing apps used to fight the pandemic. In that case the motivation to use or not use such a tool may also depends on the user's understanding of the tool [44].

One question that has not been addressed is whether users' privacy concerns about privacy tools are unique to these type of tools or if they are the same privacy concerns that exist for non-privacy tools that process data. It is important to understand users' privacy concerns in order to be able to address them, either through assurances or through privacy preserving techniques. In this study we aim to answer the following research questions: (1) are users' privacy concerns towards privacy tools different from privacy concerns towards non-privacy tools?, (2) are the reasons for privacy concern different between these types of tools, and (3) which assurances are perceived to reduce users' privacy concerns towards privacy tools, and are these different for non-privacy tools?

To answer these questions we conducted a between-subjects experiment with 185 participants recruited on Amazon Mechanical Turk. We described and showed participants a fictitious mobile app, that processed text or image data and transformed them for use on social media platforms. We manipulated the type of tool (privacy or non-privacy) as well as the type of data (text or image) that it processed, and measured participant's privacy concerns on different dimensions. We also measured participants' perception of assurances that would reduce their privacy concerns. The results show that for a privacy tool, participants' level of perceived surveillance concern is higher than for a non-privacy tool, and that the level of perceived intrusion and secondary use of personal information concerns are the same as for a non-privacy tool. In addition, participants' reasons for privacy concerns are similar for both types of tools. With regards to assurance, the results suggest that the assurance that the tool would have no ads and that the provider would explain how the tool processes the information have an effect that depends on the type of data, with a stronger effect on image data.

2 Related Work

To the best of our knowledge, there is not much research about privacy concerns on privacy enhancing tools for social media. Closest to our work is the study by Bracamonte et al. [5], who evaluated user perception of a privacy tool for social media text, and found that privacy concern was a frequent theme of users' negative opinion about the tool. In a follow up study [4], performance expectancy (usefulness), social influence and perception of accuracy were found to be positively and privacy concerns about the tool and privacy self-efficacy were found to be negatively associated with user intentions to use a privacy sensitive information detection tool.

However, there is research about privacy enhancing tools for social media and research on privacy concerns towards privacy enhancing tools in general. Thus, we briefly discuss both areas in the following subsections.

2.1 Privacy Enhancing Tools for Social Media

There are a number of proposals to help users manage their privacy on social media, and which rely on user data as input. These proposals can often be separated by the type of data they process: text or images. For text, there are many proposals for the analysis of tweets, that is, social media text of short length. Castillo and Chen [6] propose a model to identify whether tweets reveal specific privacy leaks (pregnancy and drunkenness). Wang et al. [55] analyze tweets to classify them into different privacy categories. Similarly, Tesfay et al. [52] propose a model to identify privacy sensitive information in tweets and classify them based on the EU's GDPR. Wang et al. [56] propose a model to measure the level of sensitivity of private tweets in tweets. There are also proposals with domain specific objectives. Baron and Townsend [3] propose a tool for helping paramedics to decide if and when they should communicate information about their work to the general public via social media. The Baron-Townsend Intention-To-Tweet (BITT) decision matrix aims to help the users to elaborate their motivation to post e. g. information about an accident and assess the privacy risk for the patients to be identi-

fiable. The idea behind is that if the patients privacy is maintained, the report about an accident can warn others and benefit public safety and/or allow an exchanged and education of peers.

Closely related to contextual text recommendations is the anonymization of text data, to prevent private-attribute inference attacks. Mosallanezhad et al. [38] propose "RLTA" to anonymize text data before publishing it, while preserving the utility of the text. Li et al. [32] also present an approach to obfuscate personal attributes in text data that may lead to the identification of anonymous authors of online review data. For images, Li et al. [31] propose a tool that anonymizes photos, and use this tool to evaluate the effectiveness and user experience of the most common obfuscation techniques. Based on their evaluation, they recommend in-painting [41] and avatars, and find that blurring and pixelating do not sufficiently protect against human and machine re-identification. Hasan et al. [26] propose a model for identifying bystanders in photos, so that obfuscation can be applied to protect their privacy. Finally, there is also ObscuraCam [14], an app for obscuring images.

There are other types of tools to protect users' privacy on social media. Löbner et al. [35] propose a tool to support users choose their privacy settings. The tool suggests more suitable default settings depending on a low number of questions, which reduces users' effort in making that decision. While this could naturally restrict the visibility of a post and potentially decrease privacy intrusions by the user's social media contacts, it would still mean that the provider of the social media site could see and potentially use the posted information. Thus, we do not further elaborate on other similar approaches in this section.

2.2 Privacy Concerns Towards Privacy Enhancing Tools

There are few works that address privacy concerns towards the specific type of tool that we focus on in this study (a privacy tool for social media that takes user data as input). However, there is research on privacy concerns towards other types of PETs. Tor and JonDonym are low latency anonymity services, which redirect internet traffic to conceal a user's location (IP address). The main idea is to hide communication metadata (like who communicates with whom) to a local eavesdropper. While there has been a lot of research on Tor and JonDonym [37, 47], the large majority of it is of technical nature and does not consider the users and their perceptions. That changed with a series of papers investigating reasons for the (non-)adoption of Tor [20] and JonDonym [17]. Based on the construct of internet users' information privacy concerns [42, 43] Harborth and Pape found that trust beliefs in the anonymization service played a huge role for the adoption [18, 19]. Further work [21] indicates that the providers' reputation, aka trust in the provider, played also a major role in the users' willingness to pay for or donate to these services. In a direct comparison between Tor and Jondonym with a a mixed-method approach [22, 23] it was shown that while the basic rationale of technology use models was applicable the newly added constructs of perceived anonymity and trust improved the explanatory power. This was confirmed by the qualitative study, which also offered new concepts to consider like fear of investigations and reduced accessibility of websites. Additional research on PETs in general found that besides privacy concerns, security concerns with regards to the used PET also play a crucial role in the adoption of PETs [36].

There is also research regarding the user data itself. Balebako et al. [2] designed an app prototype for providing users information on the data shared by mobile apps and interviewed participants about their perception of the privacy app. In response to a question about accuracy, participants' answers referred to wanting to be assured of the trustworthiness of the app through the assurances of third-parties such as a trusted media source, and trusting it if the reputation of the provider was proven [2]. In a study to evaluate the methods that users rely on for their online privacy, Coopamootoo [8] reported that participants considered that the trustworthiness of PETs and reputation information from trusted third-parties were important. Schaub et al. [48] investigated browser extensions for privacy awareness and detecting and blocking third-party trackers, and evaluated their effect on participants privacy concerns towards tracking. They found that some participants exhibited privacy concerns towards the extension itself, and distrusted it or thought that it would track them. They also found that participants privacy concerns towards tracking increased as a result of the extension. Participants reported concern that the extension would gather the information, and they doubted the objective of the extension because it appeared it advertised premium features. Corner et al. [9] also investigated perception of browser add-ons for blocking third-party trackers, asking participants about their perception on the trustworthiness of the add-on. Participants reported that lack of knowledge about it made them not trust it, and were

concerned that the objective was to access their data instead. On the other hand, participants that trusted the app indicated that the reason was because of explanation of its purpose and the information that the add on gave them and because it fulfilled its objective of identifying and blocking trackers.

However, in this paper, we compared concerns and assurances between privacy and non-privacy related tools and additionally have qualitatively evaluated reasons for the users' privacy concerns.

3 Method

This section defines the underlying research questions and describes the main points of the study protocol, including the design and the execution of the experiment. The study protocol including the full questionnaire is available as supplementary material.

3.1 Research Questions

Research on user perception of PETs has established that users have privacy concerns towards these tools. Research has not investigated whether these concerns are unique or not. Privacy tools that take users' text or image data as input, detect information and (possibly) apply a transformation have obvious counterparts in non-privacy tools (e.g. tools that analyze the sentiment of social media posts or that apply face filters). Therefore, it is possible to investigate how privacy concerns towards privacy tools compare to concerns about similar non-privacy tools. We define the following research questions for this study.

- R1: Is the level of privacy concern towards privacy tools different from concern towards non-privacy tools? Is that level dependent on the type of data (text or images) that is processed?
- R2: Are the reasons for privacy concerns qualitatively different for a privacy tool than for a non-privacy tool, and for different types of data?

In addition to questions about privacy concern differences, we were also interested in how these concerns might be reduced. Therefore, we also investigate the following research question.

- R3: Which type of assurances do participants think will reduce their privacy concerns? Is this perception affected by the type of tool and the type of data?

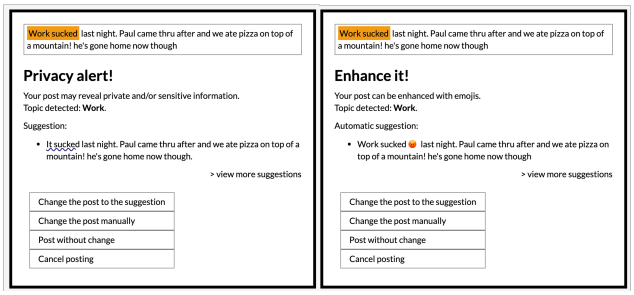
To address the research questions, we designed a between-subjects factorial experiment with two factors. The experiment was designed to test the priming effect of the type of tool and data. We defined a *Tool type* factor, with the levels *Non-privacy tool* and *Privacy tool*, and a *Data type* factor, with the levels *Text* and *Image*. The combination resulted in 4 experimental conditions.

3.2 Interface Development

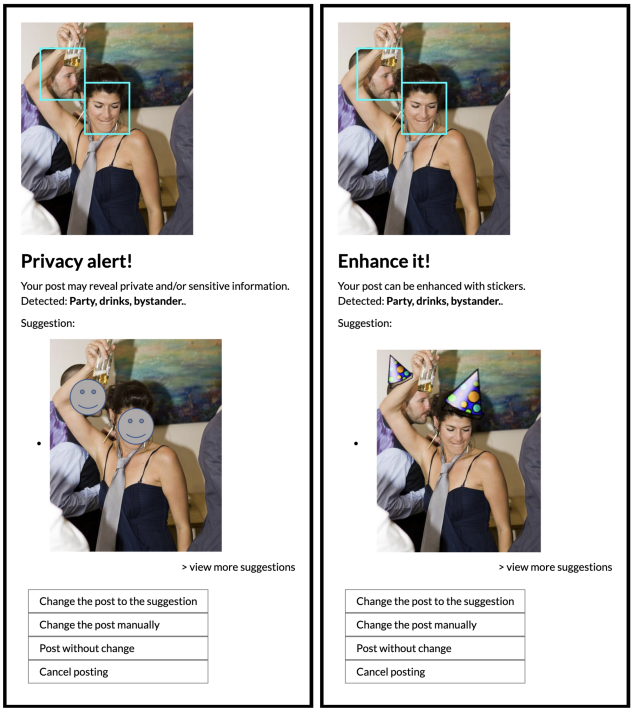
To test the effect of the tool and data type factors on privacy concerns, we developed the interface of a fictitious tool. We defined the characteristics of the tool taking into consideration that its content input, transformation and output should be as similar as possible for all experimental conditions. We also determined that the tool would be described as a mobile app to participants, as apps similar to the non-privacy app described in the study currently exist and many privacy tools are proposed as mobile apps. However, we kept the interface design close to a rough prototype, since aesthetics can have an influence on user perception [34]. The interface was progressively refined; Figure 1a, for text data, and Figure 1b, for image data, show the final version.

The interface structure was divided into detection, inference and transformation sections. The detection section consisted of an example of content (text or image), with highlighted information. For text, we highlighted phrases referring to potentially privacy sensitive topics. For images, we highlighted people's faces. In the inference section, the tool then showed a message and the topic(s) detected, and showed a suggestion of how this content could be transformed. In the transformation section, we chose to obfuscate the content, an approach taken by existing proposals for preserving privacy [24, 31].

For the text content, the privacy tool removed references to the topic in the highlight, and the non-privacy tool added a relevant emoji after the highlight. For the image content, the privacy tool obscured the faces with a grey smiley sticker, and the non-privacy tool added a sticker above the faces. We chose to obscure the faces with a sticker rather than masking with a solid box to make the transformations in both types of tools more comparable, and because masking is not preferred by users [31]. Finally, the interface showed the options a



(a) Interface for text data. Left: Privacy tool. Right: Non-privacy tool.



(b) Interface for image data. Left: Privacy tool. Right: Non-privacy tool.

Fig. 1. Tool interface for the experiment.

user could choose for their content. The text content was obtained from Sentiment140 [13], a dataset collected from Twitter. We chose the dataset for the short length of texts, easier for participants to read, and because text-based privacy tools have also targeted this type of texts [52, 56]

The image content was obtained from COCO [33], a dataset of photos of common scenes and objects, including people. We searched the datasets for content related to topics identified as private or sensitive by existing research [52, 55]. Since the same content would be shown for the *Privacy tool* and the *Non-privacy tool* levels, we chose moderately private or sensitive content that would not be completely inappropriate for a non-privacy app.

3.3 Task

In the survey, we instructed participants to imagine a scenario where there is a mobile app that can automatically analyze the content that they want to post on social media ("texts" or "photos"). We indicated that the purpose of the app was either to "protect your privacy" (privacy level) or "enhance them for fun" (non-privacy level). The instructions explained that if the app detects that the content contains information that "could be private or sensitive" or "could be enhanced", it shows a message and gives a suggestion. We indicated that the user had the option to change the content to the suggestion, make changes manually, make no changes or cancel posting. In addition, we indicated that the app was free, was not associated with a social media site (third-party) and that use of the app was voluntary not obligatory. We then showed participants the interface, and 5 examples of content and how the app would highlight it, and instructed participants to imagine that they could post similar content about themselves or about people the they know.

3.3.1 Ethical Considerations

Our institution's ethics board has a process for deciding whether a study qualifies as exempt of ethics reviews. The criteria for exemption includes non-medical, non-invasive questionnaire-based research on non-sensitive topics, and our study fell under this qualification. In addition, we provided participants with the following information. We listed the task on Amazon Mechanical Turk with the description of "Give your opinion about an app for social media content" and indicated the approximate time to finish the survey. In the introduction to the task, we included a "note before you start" indicating that the answers would be used in academic research and the instructions on how to answer, after which we included the link to the survey proper. In the survey landing page, we informed participants about the inclusion of an attention question and about the criteria for rejection (bots, unrelated answers). We did not save respondents' IP addresses. We included a notice that the data would be used in academic research but we did not include a notice on data storage. We did not explicitly mention withdrawal. Finally, we included an open-ended question for feedback and the contact information for the principal researcher at the end of the survey. Participants were from the US. In addition, we did not collect personal information, with the excep-

tion of Amazon Mechanical Turk worker ids, which were necessary to reward participants. The data was then de-identified by removing the worker ids. The data was collected in the United States and analyzed in Japan, thus the European General Data Protection Regulation was not applicable.

3.4 Questionnaire

We measured privacy concern using the Mobile users' information privacy concerns (MUIPC) scale [59], which was adapted from the Concern for Information Privacy scale [50] to address mobile users' concerns. The scale considers three dimensions of privacy concern: *Perceived surveillance* [59], *Perceived intrusion* [60], *Secondary use of personal information* [50]. We adapted these items to the scenario in our study (Table 1). The items were measured on a 7-point scale from *Strongly disagree* to *Strongly agree*. We also included a follow-up open-ended question (*"Please explain your reasons for agreeing/disagreeing to the previous questions on privacy concerns about the app."*).

For measuring the perception of how much would certain assurances reduce privacy concern, we included the question *"Please indicate how much would the following privacy assurances and/or provider would reduce your privacy concerns about the app introduced in this survey."* that applied to different types of assurances (Table 2). The types of assurances were obtained from previous research: assurances related to the type of provider [28], related to ads [54], related to institutional assurances stated in privacy policies [61], and related to how the data is processed [29]. The items were measured on a 7-point scale from *"Would not lower my privacy concerns at all"* to *"Would completely erase my privacy concerns"*.

In addition, we included single-item questions about intention (*"I would use this app in my daily life."*) and willingness to recommend the app (*"I would recommend this app to people I know."*), and about satisfaction in the transformation performed by the app. This last item was adapted from Hasan et al. [25]. We included items to characterize the sample: Prior privacy experience [50], Disposition to value privacy [61], items to measure the frequency of posting text/photos on social media, and demographic (age and gender) questions. The questionnaire also included an attention question.

3.5 Survey Pretest and Text/Image Content Validation

We conducted two pretests on the survey, first during an internal workshop with privacy research experts and then with a small number of workers on Amazon Mechanical Turk. In the workshop, we received feedback on questionnaire items, the interface, and the text and image examples that were used in the survey. We calculated an average response time of 10 minutes. A revised version was then pretested with 20 Amazon Mechanical Turk workers. We used the same recruitment conditions and compensation as for the main test, explained in the next section. We additionally compensated workers with a US$1.00 bonus for giving feedback on the survey.

The pretest included questions about the appropriateness of the examples (*"The examples of social media posts were appropriate to explain the purpose of the app"*) on a 7-point scale from *Strongly disagree* to *Strongly agree*. For the *Image* level, the mean was 6.0 , sd=0.54; for the *Text* level, the mean was 5.9, sd=0.74. In addition, we asked participants about the sensitivity of the five examples of text and image content used in the survey (*"Please imagine that the following social media posts are about you or about people you know. With that in mind, how private and/or sensitive do you think the content is?"*), rated on a 7-point scale from *"Not at all"* to *"Very much"*. For the text examples, the means ranged from 3.2 (sd = 1.75) to 4.9 (sd = 2.38); for the image examples, the mean ranged from 4.2 (sd = 1.62) to 5 (sd = 0.71). This validated that the content was considered moderately sensitive. Finally, we validated that the average time for completing the survey was 10 minutes.

3.6 Participant Recruitment

We recruited participants for our survey using the Amazon Mechanical Turk platform. We limited participation to workers from the USA, who had completed at least 1000 HITs and had a 99% worker approval rating. We set the compensation for participants at US$1.7 for the 10 minute survey, which results in a US$10.20 hourly rate. The survey ran from August 12-13, 2021.

	Measurement Items
PS1	I believe that the location of my mobile device would be monitored at least part of the time by the app.
PS2	I am concerned that the app could be collecting too much information about me.
PS3	I am concerned that the app could monitor my activities on my mobile device.
PI1	I feel that as a result of my using the app, others would know about me more than I am comfortable with.
PI2	I believe that as a result of my using the app, information about me that I consider private would be more readily available to others than I would want.
PI3	I feel that as a result of my using the app, information about me would be out there that, if used, will invade my privacy.
SU1	I am concerned that the app could use my personal information for other purposes without notifying me or getting my authorization.
SU2	When I give personal information to use the app, I am concerned that it could use my information for other purposes.
SU3	I am concerned that the app could share my personal information with other entities without getting my authorization.

Table 1. Privacy concern dimensions. PS: Perceived surveillance PI: Perceived intrusion SU: Secondary use of information

	Measurement Items
For-profit	The provider is a reputable for-profit company.
Non-profit	The provider is a non-profit organization.
Academic	The provider is an academic organization.
Data use	The provider's privacy policy says that they will only use your data for improving the app.
No ads	The app doesn't have ads.
No 3rd parties	The provider's privacy policy says that they will not sell your data to third parties.
Laws/Regulation	The provider's privacy policy says that they follow laws and regulation for personal data protection.
Client-side processing	Your data is processed in your own mobile device, and not sent to the provider.
Untraceable data	Your data is processed so that it cannot be traced back to you.
Process explanation	The provider explains how the app analyzes your content to detect and transform it.

Table 2. Assurances measurement items.

4 Results

In this section we first describe the sample obtained. We then address the main research questions of the study by comparing the experimental factors' effect on the privacy concern dimensions, quantitatively and qualitatively. Finally, we analyze the perception of assurances.

4.1 Sample Validation

We collected a total of 250 responses from Amazon Mechanical Turk workers. We identified 45 invalid responses: workers with duplicated responses, and those who had written a completely unrelated answer to the attention question. These responses were rejected; the remaining 205 participants were compensated for answering the survey. We then reviewed the answers to the attention question and frequency of social media posting; we removed from analysis 12 participant who failed the attention question and 8 participants that indicated they never posted on social media. The final sample consisted of 185 responses. The number of responses per condition was *Privacy - Text* condition, 48; *Privacy - Image* condition, 51; *Non-privacy - Text* condition, 41; and *Non-privacy - Image* condition, 45 responses.

4.2 Participant Characteristics

4.2.1 Demographics

The self-reported gender distribution of participants was 64 (36%) female, 119 (64%) male, 1 non-binary and 1 NA. The participant ages were: between 18-19, 2 (1%); between 20-29, 36 (19%); between 30-39, 17 (51%); between 40-49: 33 (18%); between 50-59, 17 (9%); and between 60-69, 2 (1%). The participants' reported frequency of social media text posting had a mean = 4.56, sd = 1.94, with a median of 5 (*"Once a week"*). Image posting frequency had a mean = 3.76, sd=1.93, with a median of 4 (*"Multiple times in a month"*).

4.2.2 Privacy Experience and Value

We analyzed responses to the *Prior privacy experience* items separately, because the scale addresses both personal experience and information, and we were interested in characterizing our sample on both of these aspects. The frequency of personally experienced incidents had a mean = 3.34, sd = 1.6, median = 3 (*"Infrequently"*). The frequency of hearing or reading about information misuse had a mean = 4.72, sd =1.53, median = 5 (*"Sometimes"*). The frequency of personally being a victim of privacy invasion had a mean = 3.24, sd = 1.69, median = 3 (*"Infrequently"*). For *Disposition to value privacy*, we summed the scores of the scale and calculated a mean = 14.37, sd = 4.75, with a median = 15. A one-sample t-test indicated that the mean was significantly higher than the middle of the scale (neutral point). To summarize, on average the participants in our sample reported that they had not frequently been affected by privacy invasion incidents, but that they had sometimes heard or read about them, and they reported a higher than neutral disposition to value the privacy of their personal information.

4.2.3 Interest and Satisfaction

Participants' intention to use the apps had a mean = 3.87, sd = 1.97, median = 4 (*"Neither"*), and their willingness to recommend the app had a mean = 4.31, sd = 1.95, median = 5 (*"Somewhat agree"*). Participants' satisfaction with the apps' transformation had a mean = 4.54, sd = 1.68, median = 5 (*"Somewhat agree"*). The non-parametrical Kruskal–Wallis test conducted on the single-item measures showed no significant differences between the privacy and non-privacy apps, text or image, for any of these variables. In general, participants' had a neutral to somewhat positive perception of the apps, and were somewhat satisfied with the transformation.

4.3 Privacy Concerns

To address the research question of whether the level of privacy concern was different among conditions (R1), we quantitatively analyzed the responses to the questions of privacy concern dimension constructs. We first measured the reliability of the privacy concern dimensions' scales with Cronbach's alpha: *Perceived surveillance* had an alpha = 0.91; *Perceived intrusion* had an alpha = 0.96; and *Secondary use of personal information* had an alpha = 0.97. All values indicate good reliability and we summed the scores for the analysis.

The separate 2x2 ANOVA on the privacy concern dimensions revealed a significant main effect of the *Tool type* level on *Perceived surveillance* $F = 4.77$, $p = 0.03$, $\eta_p^2 = 0.03$ (small effect size); but no main effect of the *Data type* level and no significant interaction. *Perceived surveillance* concern was significantly higher for the privacy tool than for the non-privacy tool (Figure 2). On the other hand, there were no significant effects on *Perceived intrusion* and *Secondary use of personal information*. The detail of the ANOVA results are shown in Table 4, and the means and standard deviation of the privacy concern dimensions are shown in 3.

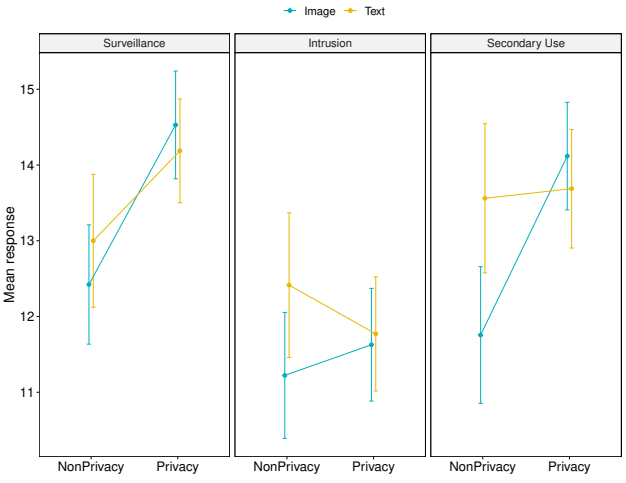


Fig. 2. Interaction plots (mean and standard error) for the privacy concerns dimensions. Higher values indicate more concern.

The results indicate that participants have a higher level of concern about their data being collected, and being tracked and monitored by the privacy tool than by the non-privacy tool. On the other hand, participants have the same level of concern about a possible invasion of privacy and about their personal information being shared and misused by the privacy tool as for the non-privacy tool. In addition, those levels of privacy concern are not different whether the tool processes text or image data.

4.4 Reasons for Privacy Concerns

To address the research question of whether the reasons for privacy concern were different (R2), we qualitatively

		Perceived surveillance		Perceived intrusion		Secondary use of personal info.	
		Mean	sd	Mean	sd	Mean	sd
Privacy tool	Text	14.19	4.75	11.77	5.22	13.69	5.43
	Image	14.53	5.08	11.63	5.31	14.12	5.07
Non-privacy tool	Text	13.00	5.62	12.42	6.12	13.56	6.31
	Image	12.42	5.28	11.22	5.58	11.76	6.05

Table 3. Mean and standard deviation of the privacy concern dimensions.

	Perceived surveillance		Perceived intrusion		Secondary use of personal info.	
	F-value	p-value	F-value	p-value	F-value	p-value
Tool type	4.771	0.030 *	0.015	0.904	2.353	0.127
Data type	0.013	0.911	0.598	0.440	0.527	0.469
Tool x Data	0.363	0.547	0.412	0.522	1.770	0.185

Table 4. 2x2 ANOVA results for the effect of Tool type and Data type on the privacy concern dimensions. * indicates significant p-value ($p < 0.05$).

analyzed the responses to the open-ended question that asked participants to explain their privacy concerns. We first excluded cases with blank answers and responses such as "none", "nothing" and similar. Removing these resulted in a total of 174 answers: *Privacy - Text* condition, 46 answers; *Privacy - Image* condition, 48 answers; *Non-privacy - Text* condition, 38 answers; *Non-privacy - Image*, 42 answers.

The process we used to analyze the answers was adapted from the general inductive approach [53], where the "data analysis is guided by the evaluation objectives". One evaluator reviewed all answers to gain understanding of the reasons and themes included in them. The evaluator identified and defined the categories based on the study questions and on existing privacy research, and created the initial codebook. The codebook was explained and discussed with two coders, who used it to code all answers independently. Many of the participants' answers referred to multiple themes simultaneously, so each answer was assigned one or multiple categories. We then calculated the inter-rater reliability. Inter-rater reliability indices apply to one-to-one categorization, that is, mutually exclusive categories per answer. Therefore, for the multiple categories, we used the approach to calculate Cohen's kappa separately for the presence/absence of each category as multiple variables [15].

The initial coding resulted in low agreement between the two coders for some categories, as well as proposals for new categories, so we conducted a second round of discussions of the codebook. As a result, we updated the codebook and the two coders recoded the answers. The results showed low agreement on the *No concern* category, and we conducted a final review to resolve the differences on that category. The average Cohen's kappa was 0.65 and the median was 0.66. A value over 0.6 indicates a substantial agreement [30], and this level of agreement applied to the majority of categories. The only case where the level of agreement was slight (< 0.2) was for the *"Know about me"* category. After the process to resolve the disagreements, the remaining comments where there was still no resolution or agreement between the coders were not used to drive the qualitative analysis or discussion.

We further classified the categories into subconcepts and concepts. Table 5 shows the categories, with example quotes from the Privacy ("PET") and Non-privacy ("Fun") levels. The result of the analysis shows that, with one exception, participants referred to similar concepts in their answers for both types of tools. We focused on the similarities and differences at the tool type level, since we did not identify clear differences at the data type level. We have mapped our findings to the three concepts "Beliefs and attitudes", "Privacy and security concerns", and "Need for assurances" and describe our categorization in the next subsections.

Concepts	Subconcepts	Common to both tools	Specific for Privacy-tool
Beliefs & attitudes	Trust	Institutional (dis)trust (Fun1, PET1); Tool (dis)trust (Fun2, PET2)	
	Privacy mindset	General privacy concern (Fun3, PET3); No concern (Fun4,PET4); Gave up on privacy (Fun1, Fun3, PET1); Perception of profit motivation (Fun5, PET5)	
	Perceived control	Nothing to hide (Fun6,PET6); Self-efficacy (Fun7, PET7); Limited information (Fun8, PET8); Avoidance of unnecessary apps (Fun9, PET9)	Privacy objective of the tool (PET17)
Privacy & security concerns	Surveillance	Data collection (Fun10, PET10); Tracking (Fun11, PET11)	
	Intrusion	Know about me (Fun12, PET12)	
	Secondary use	Sell/share data (Fun13, Fun12, PET10); Data misuse (Fun14, PET10)	
	Security risks	Security risks (Fun1,PET13)	
Need for assurances	Technical	Data processing (Fun15, PET14); Tool permissions (Fun16, PET15)	
	Information	Unknown reputation (Fun17, PET16); No information about the tool (Fun18, PET15)	

Fun1 *"[...] it's standard for either companies to sell data or get hacked. I get the concern, but in my opinion it just comes with the territory."*
Fun2 *"i would trust that the app would not share my personal information"*
Fun3 *"I always have privacy concerns. but there's not much you can really do about it."*
Fun4 *"I have no privacy concerns, it's just not my style of app"*
Fun5 *"The app is also free so that could be how they make money."*
Fun6 *"I take a stance of I have nothing to hide."*
Fun7 *"I am not concerned about privacy because I usually am careful about what I put on apps."*
Fun8 *"It won't ask for sensitive details such as bank information, house address e.t.c [...]"*
Fun9 *"I dont trust a lot of apps. i try to keep my downloading of apps to a minimum"*
Fun10 *"If an application gathers more about the personal information about me I would not likely to use the app further"*
Fun11 *"I think that the app would track your content [...]"*
Fun12 *"They can find out so much about you and sell the info."*
Fun13 *"All apps use information for them to work, the makers of the apps sell this information or use it for marketing."*
Fun14 *"I'm also concerned that the app might use information to advertise to me [...]"*
Fun15 *"I do have privacy concerns as I would want to know what happens to the text that the app analyzes."*
Fun16 *"Im sure you can set your preferences in regard to privacy."*
Fun17 *"I would like to know about the developer"*
Fun18 *"I would need to read the privacy policy before I can answer one way or another."*

PET1 *"I think there is a privacy concern with almost every website or app we use today but after awhile you just stop caring"*
PET2 *"It is difficult to totally trust the app not to expose my personal details."*
PET3 *"These are the same privacy concerns I would have about any app"*
PET4 *"I don't care about privacy concerns."*
PET5 *"[...] the fact that it's free does make me worry that it might sell my information to ad services to generate revenue."*
PET6 *"[...] but I also don't have a life that needs to be censored."*
PET7 *"I believe at first, I decide the kind of information to post on the app;"*
PET8 *"The app appears to only look at trigger words and phrases [...]"*
PET9 *"I don't need yet another app [...] I'd rather limit the amount of data that is already out there, not create more."*
PET10 *"The data gained by the app could be shared with other organizations to offer me certain services or products which I dislike."*
PET11 *"I think it is very difficult nowadays to use apps [...] without being tracked at least in some way."*
PET12 *"the app will get an idea about my characteristics, routine etc. which can be sold [...]"*
PET13 *"[...] there is an inherent risk of data being leaked [...]"*
PET14 *"[...] it's an automated system and I don't think a real person would review it."*
PET15 *"I would want to know what information was shared and for what purpose. I would want opportunity to opt out or authorize information."*
PET16 *"I don't know the maker of the app [...]"*
PET17 *"[...] the whole purpose of the app is to maintain privacy and therefore I am not really concerned about the app misusing my information."*

Table 5. Results of the coding of the answer to the open-ended question, including quotes. PET: Privacy tool. Fun: Non-privacy tool.

4.4.1 Beliefs and Attitudes

This concept refers to comments that indicated beliefs or attitudes of the participants.

Trust

Answers for the subconcept of *Trust* were the most frequent answers. In particular the *Institutional (dis)trust*, described answers that painted all apps or providers, that is, the app ecosystem, as trustworthy or untrustworthy (**Fun1**). We can gather from the answers in this category that participants' trust and distrust apply to the privacy tool regardless of its stated objective. A participant in the privacy tool condition indicated: *"I don't trust any company with my personal information. [...]"*. The *Tool (dis)trust* category described answers where participants claim to either trust or distrust the tool but did not make generalizations to other apps (**Fun2**, **PET2**). We considered both trust and distrust in both of these categories, but answers that evidenced distrust were more frequent. This type of answer was often found together with the participants' specific concern aspects such as the collection, selling and misuse of data. Trusting and distrusting comments were balanced regardless of the tools' objective and there was no clear tendency visible.

Privacy Mindset

General privacy concerns (**Fun3**, **PET3**) and *No concerns* (**Fun4**, **PET4**) describe answers where participants indicated that they have or have no privacy concerns in general. *Gave up on privacy* describes answers where participants have resigned to the state of privacy violations (**PET1**). Participants are aware that privacy violations exist, but feel that they cannot do anything about them. Furthermore, we found several comments from the participants about the expected business model of the proposed tool, namely the *Perception of profit motivation* for the privacy tool as well as for the non-privacy tool. Participants were worried that since the tool was said to be free, the only way to make revenue would be to sell their data (**Fun5**, **PET5**).

Perceived Control

Some participants referred to how they managed or expected to manage privacy risk in their answers. We named this concept perceived control as it is not clear per se if the participants' approach is really effective. As the name indicates, *Nothing to hide* described answers where participants' did not consider that their information needed to be kept private at all (**Fun6**, **PET6**). *Self-efficacy* describes answers that reflected participants self-perceived ability to avoid privacy risks (**Fun7**, **PET7**). *Limited information taken by the tool* describes answers that showed participants' assumptions about the type of information that the tool would require and concluding that this would limit possible privacy violations (**Fun8**, **PET8**). *Avoidance of unnecessary apps* describes answers where the participants explained that they try to have a minimum number for apps (**Fun9**, **PET9**). Often this comment was connected with the participants' concerns that their data was sold or shared and/or the comment that they do not need a tool like this (holds for the privacy and non-privacy tool). Finally, the *Privacy objective of the tool* was the only category that applied to the privacy tool exclusively. Some participants indicated that they were not concerned about their privacy because the tool objective was to protect their privacy (**PET17**).

4.4.2 Privacy and Security Concerns

This concept refers to privacy and security concerns towards the app or its providers (in contrast to general privacy concerns or no privacy concerns from the privacy mindset subconcept). For the privacy tool, the answers touched upon the same concerns as for the non-privacy tool: that the data would be gathered and sold to be used without the users' approval.

Surveillance

Participants were concerned about the *Data collection* of the tool in general (**Fun10**), and the privacy tool was also a source of this concern: *"Although the app would prevent personal information from being publicly published, the app itself would have a "database" of information [...]"*. They also specifically referred to the possibility of the tool *Tracking* them, i.e. their location (**Fun11**, **PET11**).

Intrusion

The *Know about me* category described participants concerns about intrusion, although these were less frequent. Participants were concerned that that the tool would know about their "characteristics, routine" (**PET12**),

although they did not always mention possible misuse of this knowledge.

Secondary Use

The categories *Data misuse* (**Fun14**, **PET10**) and *Sell/share data* (**Fun13**) similarly applied to both types of tools. Referring to the privacy tool, a participant indicated that their privacy concern was *"Because all apps seem to take data and sell them for money."*. And a participant in the Non-privacy level indicated *"all apps do this. they all collect information and sell it. nothing is free"*. These two categories were often found together with *Data collection* in the same answer. Participants were concerned that their data would be used for other things than the tools' primary purposes.

Security Risks

In addition, there were also answers that we categorized as *Security risks*, which described concern about the possibility of hacking or leaks (**PET13**).

4.4.3 Need for Assurances

This concept groups answers that related to participants' request for details about the tool and the provider.

Technical

Technical categories referred to questions about how *Data processing* was conducted (**Fun15**, **PET14**), or the type of *Tool permissions* that existed to control access to data in the mobile device (**Fun16**, **PET15**).

Information

In the *Information* categories, the *Unknown reputation* category consisted of answers that mentioned requiring more information about the provider or from other sources regarding the trustworthiness of the tool (**Fun17**, **PET16**). We did not provide information about the fictitious provider beyond stating that it would not be the social media site, so we had expected that participants' concerns would be related to questions about reputation, but relatively few answers fell under this category. Finally, the *No information about the tool* category referred to participant's request or need to know more about the tool, such as it's privacy policy (**Fun18**), or in general. For the privacy tool, a participant indicated that *"(they) didn't see any information about their rules on data sharing"*.

4.5 Perception of Assurances

To address the research question of whether assurances are perceived to reduce participants' privacy concerns (R3), we conducted separate 2x2 ANOVA for the each of assurance types. The results showed no significant main effect of tool type or data type on any of the assurance types, but there was a significant interaction effect on the *No ads* assurance, $F = 4.018$, $p = 0.047$, $\eta_p^2 = 0.02$ (small effect size) and on the *Process explanation* assurance, $F = 6.169$, $p = 0.014$, $\eta_p^2 = 0.03$ (small effect size). Table 7 shows the detail of the results for the *No ads* and *Process explanation* assurances. The post hoc Sidak-adjusted pairwise mean comparison showed no significant differences between each condition for either of the assurances, which may be due to low power of the test. The non-significant comparisons difficult the interpretation of results, but we report the conditions with the largest difference for reference. For the *Process explanation* assurance, the contrast between the *Non-privacy tool - Image* and *Privacy tool - Image* conditions had the largest difference with an estimate = -0.889, SE = 0.35, p = 0.058. Figure 3 shows the interaction plots.

Next, we conducted separate one-sample t-tests to evaluate if the means were significantly higher from the neutral score of 3, that is if participants thought these assurances would reduce their privacy concerns. All results were significant with a Bonferroni-adjusted $p < .001$. Table 6 shows the means for all assurances by condition. The results show that participants considered that all types of assurances presented would reduce their privacy concern to some extent or other.

As Figure 3 illustrates, assurances related to data processing (that the data would be processed client-side and that the user data cannot be traced back to them) were the ones with higher means, that is, that participants thought would reduce their privacy concerns more. Next were the assurances that the provider would provide explanation about how the app analyzes the data and that the data would not be sold.

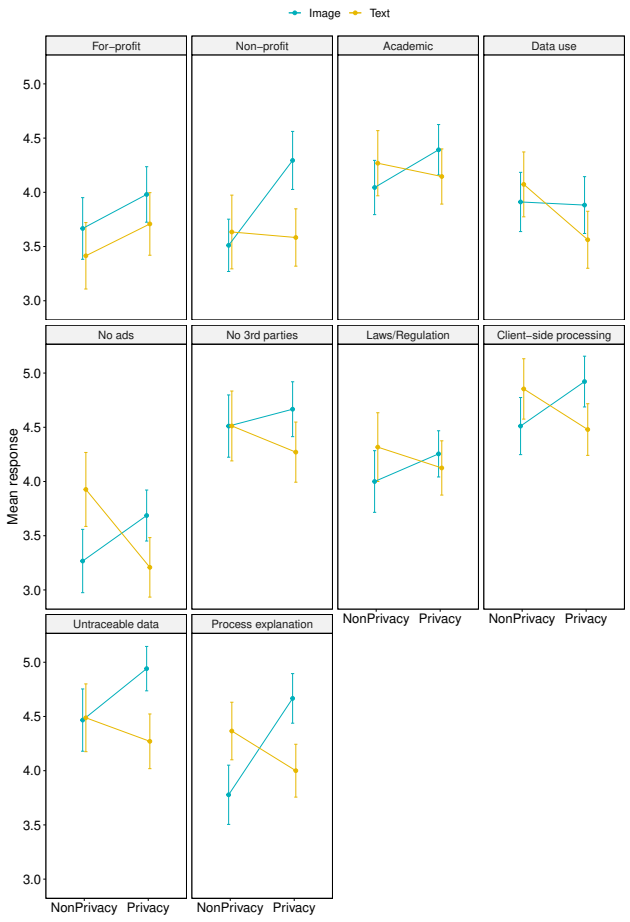


Fig. 3. Interaction plots (mean and standard error) for perception of assurances. Higher values indicate a stronger perception that the assurance would reduce privacy concerns.

	Privacy tool		Non-privacy tool	
	Text	Image	Text	Image
For-profit	3.71	3.98	3.42	3.67
Non-profit	3.58	4.29	3.63	3.51
Academic	4.15	4.39	4.27	4.04
Data use	3.56	3.88	4.07	3.91
No ads	3.21	3.69	3.93	3.27
No 3rd parties	4.27	4.67	4.51	4.51
Laws/Regulation	4.13	4.26	4.32	4.00
Client-side processing	4.48	4.92	4.85	4.51
Untraceable data	4.27	4.94	4.49	4.47
Process explanation	4.00	4.67	4.37	3.78

Table 6. Mean of assurances items per experimental condition.

	No ads		Process explanation	
	F-value	p-value	F-value	p-value
Tool type	0.201	0.654	1.284	0.259
Data type	0.032	0.858	0.111	0.740
Tool x Data	4.017	0.047 *	6.169	0.014 *

Table 7. 2x2 ANOVA results for the effect of Tool type and Data type on the perception of No ads and Process explanation assurances.
* indicates significant p-value ($p<.05$).

5 Discussion

Taken as a whole, the results of the study suggest a negative situation for privacy tools. At best, participants have the same level of privacy concerns towards privacy tools than towards non-privacy tools. At worst, participants report more concern that the privacy tools will collect their personal information and monitor their behavior, compared to non privacy tools. That is, that the priming effect of the privacy purpose of the tool is an increase in perceived surveillance concern.

On the other hand, the reasons that participants give for their privacy concern towards both tools are very similar. In particular, the frequent mentions of institutional distrust towards the app ecosystem indicate that the current widespread situation of online data collection, selling and use (in particular for ad revenue) negatively affects all types of tools. The quantitative results show that the level of perceived surveillance concern was higher for the privacy tool, but we did not find that the reasons reported in the open-ended questions clearly explained why there was a difference. Xu et al. [59] indicates that *Perceived surveillance* pertains specifically to the act of collecting the data, but the answers that mentioned data collection were similar in number as those that mentioned selling or sharing of data and data misuse, for both types of tools. The analysis of the assurances that participants' thought would lower their privacy concerns also do not offer hints for the difference in surveillance concern. However, we note one of the assurances that was most positively perceived was related to the data collection aspect: the assurance that the data would remain in the device. We showed that both types of tools take the same data as input and process it in a similar way (detecting some information and transforming the content) and therefore the difference likely comes from the priming effect of the privacy objective of the tool, but we lack information to clearly state why this affects the surveillance dimension and not the others. Future research should investigate in detail the reasons for the differences found.

Expectations on the Tool Provider's Business Model

Comments about privacy concerns because the tools have been announced to be free are in line with observations from Han et al. [16] who found that consumers expect paid apps to have better security and privacy behaviors than their free counterparts. However, in the same paper it was also stated that there is no clear evidence that paying for an app will avoid extensive data collection in practice since often the paid and free version of the app share a common code base including third-party libraries and requesting dangerous permissions. Thus, this might be a misperception on the users' side.

Relation between Concerns and Assurances

The observation that the level of privacy concern was rather high is reflected by finding frequent comments on all three dimensions of the MUIPC scale used to measure the privacy concerns: Perceived surveillance, Perceived intrusion, and secondary use. There were also comments that addressed concerns regarding Security risks, Perceived control, and Trust. We found comments on the expected business model (free versus paid tools), about the processing of the data which could be mapped to process explanation and client-side processing, which relate to the assurances that we investigate in this study. However, we also found comments related to the assumption that the tool provides permissions and on the reputation of the provider, which were not included in the list of assurances. This suggests that further research could focus on the influence of other types of control assurances on privacy concerns.

Privacy-by-Design for Privacy Tools

The qualitative answers show that there are participants that give the benefit of the doubt due to the privacy objective of the tool. Emphasis on the privacy objective, in combination with assurances such as being clear who provides the app, may help reduce privacy concerns in some participants. However, a strong reason for participants' concerns was their perception of the state of app ecosystem with regards to the selling, sharing and misuse of data. And participants' report that assurances related to how their data is processed would reduce their concern.

Unfortunately, proposals for privacy tools do not often include discussions of how users' data would be protected. Naturally, researchers do not assume that they would themselves misuse the personal information, but as participants' indicate, there are hacking and leakage security risks.

From a technical point of view, the data processing of the privacy tools described in our study does not differ from the non-privacy tools. Therefore, one way to address this issue is to use techniques that maintain the privacy of the data being processed, and to design the privacy tools in a way that minimizes data collection and storage. While privacy by design [7] can help with the implementation, privacy preserving techniques, such as Federated Learning [58], Homomorphic Encryption [45], Secure Multiparty Computation [46] or Differential Privacy [11] can be used to ensure technically that the user data stays private. These efforts are not trivial, as these techniques can affect the performance and implementation costs of the solutions Bagdasaryan et al. [1].

In addition, data privacy preserving techniques can be difficult to communicate to users, who may not grasp the technical details. Thus, it is important to educate the users about the tool and explain them how it works. A recent study [44] on the German contact tracing app (Corona Warn App) asked participants of a survey four questions about the Corona Warn App and compared it with their privacy concerns. Since the Corona Warning App was designed with privacy in mind, non surprisingly those who could answer three or all four questions correctly had significantly less privacy concerns than participants with a lower number of correct answers. However, since there was also a correlation between users of the Corona Warn App and knowledge about the app, the question of causality is still open: Are users more knowing and have less privacy concerns because they use the app or do knowing users have less privacy concerns, and thus use the app?

5.1 Limitations

The study has a number of limitations. The main limitation is related to the generalizability of results. We used a fictitious app and only showed an interface screenshot. Although many proposals for privacy tools such as the one we describe exist, there are no implementations that we could use while controlling for factors such as provider and the effect of design aesthetic. Nevertheless, this limits how believable the scenario is for the participants, and their responses may be different for real apps. Another barrier to generalizability is the content used for the examples of how the tool would work. We used text and images from publicly available datasets,

so there is a limit to how strongly participants may have associated that content with content they would post themselves, and this could have biased the results. We did not follow an ideal process for informed consent, as we did not include mention of the possibility of withdrawing from the study, and did not mention how the participants' data would be handled. We did not include ethnicity or other demographic questions besides age and gender, and we did not analyze whether the results were dependent on these characteristics. Finally, we recruited participants from Amazon Mechanical Turk, which may have introduced bias. Amazon Mechanical Turk works have a have been reported as likely to use social media, but they are also reported to have higher privacy concerns [27].

6 Conclusion

Although the fact that users have concerns towards privacy tools that process user data has been reported in evaluation of these tools, no studies have addressed whether the issue is unique to the privacy tools or the same as for other tools that process user data. In this study, we addressed the question of whether these concerns are different, by conducting an experiment and analyzing the results quantitatively and qualitatively. The results showed that privacy tools appear to be at disadvantage: for the dimension of perceived surveillance, participants report a higher level of concern than for the non-privacy tools. And for dimensions of perceived intrusion and secondary use of personal information concern, participants have the same level of privacy concern. In addition, the reasons for this concern are also similar, and participants' opinions on the data practices of the app ecosystem affect privacy tools as well. Finally, participants prefer assurances about data processing, which reflects their main reasons for concern. Future research in planned to investigate in more detail which type of assurances would work to reduce privacy concerns towards privacy tools.

Acknowledgements

This research was partially supported by the European Union's Horizon 2020 research and innovation program from the project CyberSec4Europe (grant agreement number 830929).

References

[1] Eugene Bagdasaryan, Omid Poursaeed, and Vitaly Shmatikov. Differential privacy has disparate impact on model accuracy. *Advances in Neural Information Processing Systems*, 32:15479–15488, 2019.

[2] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. "Little Brothers Watching You": Raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 1–11. Association for Computing Machinery, July 2013. ISBN 978-1-4503-2319-2. 10.1145/2501604.2501616.

[3] Aidan Baron and Ruth Townsend. Live tweeting by ambulance services: A growing concern. *Journal of Paramedic Practice*, 9(7):282–286, 2017.

[4] Vanessa Bracamonte, Sebastian Pape, and Shinsaku Kiyomoto. Investigating user intention to use a privacy sensitive information detection tool. In *Symposium on Cryptography and Information Security (SCIS)*, January 2021.

[5] Vanessa Bracamonte, Welderufael B. Tesfay, and Shinsaku Kiyomoto. Towards Exploring User Perception of a Privacy Sensitive Information Detection Tool. In *7th International Conference on Information Systems Security and Privacy*, 2021.

[6] Saul Ricardo Medrano Castillo and Zhiyuan Chen. Using Transfer Learning to Identify Privacy Leaks in Tweets. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, pages 506–513, November 2016. 10.1109/CIC.2016.078.

[7] Ann Cavoukian et al. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, 5:12, 2009.

[8] Kovila P.L. Coopamootoo. Usage Patterns of Privacy-Enhancing Technologies. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, pages 1371–1390. Association for Computing Machinery, October 2020. ISBN 978-1-4503-7089-9. 10.1145/3372297.3423347.

[9] Matthew Corner, Huseyin Dogan, Alexios Mylonas, and Francis Djabri. A Usability Evaluation of Privacy Add-Ons for Web Browsers. In Aaron Marcus and Wentao Wang, editors, *Design, User Experience, and Usability. Practice and Case Studies*, Lecture Notes in Computer Science, pages 442–458. Springer International Publishing, 2019. ISBN 978-3-030-23535-2. 10.1007/978-3-030-23535-2_33.

[10] Lorrie Faith Cranor and Simson Garfinkel. *Security and Usability: Designing Secure Systems That People Can Use*. " O'Reilly Media, Inc.", 2005.

[11] Natasha Fernandes, Mark Dras, and Annabelle McIver. Generalised differential privacy for text document processing. In *International Conference on Principles of Security and Trust*, pages 123–148. Springer, Cham, 2019.

[12] Kevin Gallagher, Sameer Patil, Brendan Dolan-Gavitt, Damon McCoy, and Nasir Memon. Peeling the onion's user experience layer: Examining naturalistic use of the tor browser. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1290–1305, 2018.

[13] Alec Go, Richa Bhayani, and Lei Huang. Sentiment140. *Site Functionality, 2013c. URL http://help. sentiment140. com/site-functionality. Abruf am*, 20, 2016.

[14] Guardian Project. ObscuraCam: Secure Smart Camera. URL https://guardianproject.info/apps/obscuracam/.

[15] Kevin A. Hallgren. Computing Inter-Rater Reliability for Observational Data: An Overview and Tutorial. *Tutorials in quantitative methods for psychology*, 8(1):23–34, 2012. ISSN 1913-4126.

[16] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazar, Kenneth A Bamberger, and Serge Egelman. The price is (not) right: Comparing privacy in free and paid apps. *Proceedings on Privacy Enhancing Technologies*, 2020(3), 2020.

[17] David Harborth and Sebastian Pape. Examining technology use factors of privacy-enhancing technologies: The role of perceived anonymity and trust. In *24th Americas Conference on Information Systems, AMCIS 2018, New Orleans, LA, USA, August 16-18, 2018*. Association for Information Systems, 2018. URL https://aisel.aisnet.org/amcis2018/Security/Presentations/15.

[18] David Harborth and Sebastian Pape. JonDonym users' information privacy concerns. In *ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings*, pages 170–184, 2018. 10.1007/978-3-319-99828-2_13.

[19] David Harborth and Sebastian Pape. How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies – the case of tor. In *52nd Hawaii International Conference on System Sciences (HICSS) 2019*, pages 4851–4860, January 2019. 10125/59923.

[20] David Harborth and Sebastian Pape. How privacy concerns, trust and risk beliefs and privacy literacy influence users' intentions to use privacy-enhancing technologies - the case of tor. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 51(1):51–69, January 2020. ISSN 0095-0033. 10.1145/3380799.3380805.

[21] David Harborth, Xinyuan Cai, and Sebastian Pape. Why do people pay for privacy-enhancing technologies? the case of tor and JonDonym. In *ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings*, pages 253–267, June 2019. 10.1007/978-3-030-22312-0_18.

[22] David Harborth, Sebastian Pape, and Kai Rannenberg. Explaining the technology use behavior of privacy-enhancing technologies: The case of tor and JonDonym. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020(2): 111–128, May 2020. 10.2478/popets-2020-0020.

[23] David Harborth, Sebastian Pape, and Kai Rannenberg. Explaining the technology use behavior of privacy-enhancing technologies: The case of tor and JonDonym (poster). In *17th Symposium on Usable Privacy and Security (SOUPS 2021)*, June 2021. URL https://www.usenix.org/conference/soups2021/presentation/harborth-0.

[24] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. Viewer Experience of Obscuring Scene Elements in Photos to Enhance Privacy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13. Association for Computing Machinery, April 2018. ISBN 978-1-4503-5620-6.

[25] Rakibul Hasan, Yifang Li, Eman Hassan, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. Can Privacy Be Satisfying?: On Improving Viewer Satisfaction for Privacy-Enhanced Photos Using Aesthetic Transforms. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, page 367. ACM, May 2019. ISBN 978-1-4503-5970-2. 10.1145/3290605.3300597.

[26] Rakibul Hasan, David Crandall, Mario Fritz, and Apu Kapadia. Automatically Detecting Bystanders in Photos to Reduce Privacy Risks. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 318–335, May 2020. 10.1109/SP40000.2020.00097.

[27] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 37–49, 2014. ISBN 978-1-931971-13-3.

[28] Mark J. Keith, Jeffry S. Babb, and Paul Benjamin Lowry. A Longitudinal Study of Information Privacy on Mobile Devices. In *2014 47th Hawaii International Conference on System Sciences*, pages 3149–3158, January 2014. 10.1109/HICSS.2014.391.

[29] Alfred Kobsa, Bart P. Knijnenburg, and Benjamin Livshits. Let's do it at my place instead? attitudinal and behavioral study of privacy in client-side personalization. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 81–90. Association for Computing Machinery, April 2014. ISBN 978-1-4503-2473-1. 10.1145/2556288.2557102.

[30] J. Richard Landis and Gary G. Koch. The measurement of observer agreement for categorical data. *biometrics*, pages 159–174, 1977.

[31] Yifang Li, Nishant Vishwamitra, Bart P Knijnenburg, Hongxin Hu, and Kelly Caine. Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–24, 2017.

[32] Yitong Li, Timothy Baldwin, and Trevor Cohn. Towards robust and privacy-preserving text representations. *arXiv preprint arXiv:1805.06093*, 2018.

[33] Tsung-Yi Lin, Michael Maire, Serge Belongie, James Hays, Pietro Perona, Deva Ramanan, Piotr Dollár, and C. Lawrence Zitnick. Microsoft COCO: Common Objects in Context. In David Fleet, Tomas Pajdla, Bernt Schiele, and Tinne Tuytelaars, editors, *Computer Vision – ECCV 2014*, Lecture Notes in Computer Science, pages 740–755. Springer International Publishing, 2014. ISBN 978-3-319-10602-1. 10.1007/978-3-319-10602-1_48.

[34] Gitte Lindgaard, Cathy Dudek, Devjani Sen, Livia Sumegi, and Patrick Noonan. An exploration of relations between visual appeal, trustworthiness and perceived usability of homepages. *ACM Transactions on Computer-Human Interaction*, 18(1):1:1–1:30, May 2011. ISSN 1073-0516. 10.1145/1959022.1959023.

[35] Sascha Löbner, Welderufael B. Tesfay, Toru Nakamura, and Sebastian Pape. Explainable machine learning for default privacy setting prediction. *IEEE access : practical innovations, open solutions*, 9:63700–63717, April 2021. 10.1109/ACCESS.2021.3074676.

[36] Federico Mangiò, Daniela Andreini, and Giuseppe Pedeliento. Hands off my data: Users' security concerns and intention to adopt privacy enhancing technologies. *Italian Journal of Marketing*, 2020(4):309–342, 2020.

[37] Antonio Montieri, Domenico Ciuonzo, Giuseppe Aceto, and Antonio Pescapé. Anonymity services Tor, I2P, JonDonym: Classifying in the dark. In *Teletraffic Congress (ITC 29), 2017 29th International*, volume 1, pages 81–89. IEEE, 2017.

[38] Ahmadreza Mosallanezhad, Ghazaleh Beigi, and Huan Liu. Deep reinforcement learning-based text anonymization against private-attribute inference. In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, pages 2360–2369, 2019.

[39] P. Murmann and S. Fischer-Hübner. Tools for Achieving Usable Ex Post Transparency: A Survey. *IEEE access : practical innovations, open solutions*, 5:22965–22991, 2017. ISSN 2169-3536. 10.1109/ACCESS.2017.2765539.

[40] Hoang-Quoc Nguyen-Son, Minh-Triet Tran, Hiroshi Yoshiura, Noboru Sonehara, and Isao Echizen. Anonymizing Personal Text Messages Posted in Online Social Networks and Detecting Disclosures of Personal Information. *IEICE Transactions on Information and Systems*, E98.D(1):78–88, 2015. 10.1587/transinf.2014MUP0016.

[41] José Ramón Padilla-López, Alexandros Andre Chaaraoui, Feng Gu, and Francisco Flórez-Revuelta. Visual privacy by context: Proposal and evaluation of a level-based visualisation scheme. *Sensors*, 15(6):12959–12982, 2015.

[42] Sebastian Pape, Ana Ivan, David Harborth, Toru Nakamura, Shinsaku Kiyomoto, Haruo Takasaki, and Kai Rannenberg. Re-evaluating internet users' information privacy concerns: The case in japan. *AIS Transactions on Replication Research*, 6(18):1–18, October 2020. 10.17705/1atrr.00061.

[43] Sebastian Pape, Ana Ivan, David Harborth, Toru Nakamura, Shinsaku Kiyomoto, Haruo Takasaki, and Kai Rannenberg. Open materials discourse: Re-evaluating internet users' information privacy concerns: The case in japan. *AIS Transactions on Replication Research*, 6(22):1–7, October 2020. 10.17705/1atrr.00065.

[44] Sebastian Pape, David Harborth, and Jacob Leon Kröger. Privacy concerns go hand in hand with lack of knowledge: The case of the german corona-warn-app. In A. Jųsang, L. Futcher, and J. Hagen, editors, *ICT Systems Security and Privacy Protection - 36th IFIP TC 11 International Conference, SEC 2021*, volume 625 of *IFIP Advances in Information and Communication Technology*, pages 256–269. Springer, March 2021. 10.1007/978-3-030-78120-0_17.

[45] Payal V Parmar, Shraddha B Padhar, Shafika N Patel, Niyatee I Bhatt, and Rutvij H Jhaveri. Survey of various homomorphic encryption algorithms and schemes. *International Journal of Computer Applications*, 91(8), 2014.

[46] Devin Reich, Ariel Todoki, Rafael Dowsley, Martine De Cock, and Anderson CA Nascimento. Privacy-preserving classification of personal text messages with secure multi-party computation: An application to hate-speech detection. *arXiv preprint arXiv:1906.02325*, 2019.

[47] Saad Saleh, Junaid Qadir, and Muhammad U. Ilyas. Shedding light on the dark corners of the internet: A survey of tor research. *Journal of Network and Computer Applications*, 114: 1–28, 2018. ISSN 1084-8045. 10.1016/j.jnca.2018.04.002.

[48] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. Watching Them Watching Me: Browser Extensions Impact on User Privacy Awareness and Concern. In *Proceedings 2016 Workshop on Usable Security*. Internet Society, 2016. ISBN 978-1-891562-42-6. 10.14722/usec.2016.23017.

[49] Manya Sleeper, Justin Cranshaw, Patrick Gage Kelley, Blase Ur, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. "i Read My Twitter the next Morning and Was Astonished": A conversational perspective on Twitter regrets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 3277–3286. Association for Computing Machinery, April 2013. ISBN 978-1-4503-1899-0. 10.1145/2470654.2466448.

[50] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2):167–196, 1996. ISSN 0276-7783. 10.2307/249477.

[51] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, July 2021. ISSN 2299-0984. 10.2478/popets-2021-0049.

[52] Welderufael B. Tesfay, Jetzabel Serna, and Kai Rannenberg. PrivacyBot: Detecting Privacy Sensitive Information in Unstructured Texts. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, pages 53–60, October 2019. 10.1109/SNAMS.2019.8931855.

[53] David R. Thomas. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2):237–246, June 2006. ISSN 1098-2140. 10.1177/1098214005283748.

[54] Na Wang, Bo Zhang, Bin Liu, and Hongxia 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*, MobileHCI '15, pages 373–382. Association for Computing Machinery, August 2015. ISBN 978-1-4503-3652-9. 10.1145/2785830.2785845.

[55] Qiaozhi Wang, Jaisneet Bhandal, Shu Huang, and Bo Luo. Classification of Private Tweets Using Tweet Content. In *2017 IEEE 11th International Conference on Semantic Computing (ICSC)*, pages 65–68, January 2017. 10.1109/ICSC.2017.36.

[56] Qiaozhi Wang, Hao Xue, Fengjun Li, Dongwon Lee, and Bo Luo. #DontTweetThis: Scoring Private Information in Social Networks. *Proceedings on Privacy Enhancing Technologies*, 2019(4):72–92, October 2019. 10.2478/popets-2019-0059.

[57] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. "I Regretted the Minute I Pressed Share": A qualitative

study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 1–16. Association for Computing Machinery, July 2011. ISBN 978-1-4503-0911-0. 10.1145/2078827.2078841.

[58] Xing Wu, Zhaowang Liang, and Jianjia Wang. Fedmed: A federated learning framework for language modeling. *Sensors*, 20(14):4048, 2020.

[59] H. Xu, Sumeet Gupta, M. Rosson, and J. Carroll. Measuring Mobile Users' Concerns for Information Privacy. In *ICIS*, 2012.

[60] Heng Xu, Tamara Dinev, H. Smith, and Paul Hart. Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *ICIS 2008 Proceedings*, January 2008.

[61] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, 12(12), December 2011. ISSN 1536-9323. 10.17705/1jais.00281.

Appendix

We describe the research objective and questions, study design, criteria for recruiting participants and the survey instrument of the present study.

Research Objective

The objective of the present study is to evaluate how privacy concerns towards privacy tools compare to concerns towards non-privacy tools. Specifically, we evaluate the following research questions:

- Is the level of privacy concern towards privacy tools different from concern towards non-privacy tools? Is that level dependent on the type of data (text or images) that is processed?
- Are the reasons for privacy concerns qualitatively different for a privacy tool than for a non-privacy tool, and for different types of data?

Study Design

To address the research questions, we designed a between-subjects factorial experiment with two factors:

• Tool type: The type of tool that processes the data, with the following levels:

- Privacy tool: the purpose of the tool is to preserve privacy.
- Non-privacy tool: the purpose of the tool is enjoyment or fun, not related to privacy.

• Data type: The type of data that the tool processes, with the following levels:

- Text: only words or characters such as emojis.
- Images: only image content such as photos.

The combination results in 4 experimental conditions.

Criteria for Participants Recruited

We used the Amazon Mechanical Turk platform to recruit participants. The task was posted on the platform as follows:

- Description: Give your opinion about an app for social media content. 10min. approx.
- Keywords: social media, content, survey

The criteria (qualifications) for participants were as follows:

- Worker approval Rate (%) greater than or equal to 99%
- Number of HITs approved greater than or equal to 1000
- Location is US

Survey Instrument

This section contains the description of the survey and questions shown to participants. The first subsection shows the description of the task and access to the survey, the second subsection shows the questionnaire itself.

Description and Access to the Survey

Amazon Mechanical Turk workers that accessed the task were shown the following information, followed by a link to the survey.

Task
Give your opinion about an app for social media content

Important
Please complete only 1 HIT. We cannot accept duplicated responses.

Note before you start:

- The answers you provide will be used in academic research.
- The survey should take around 10 minutes.
- Use a desktop computer or a laptop for this task, not a mobile device.

Instructions:

- Click on the link below to complete the survey.
- In the survey, you will be asked to input your Amazon Mechanical Turk WorkerID. Please make sure to fill it correctly.
- At the end of the survey, there will be a confirmation message with a completion code to paste into the box below.
- Make sure to leave this window open as you complete the survey. When you are finished, return to this page to paste the code into the box.

Thank you.

Survey

The following is the full survey for the study. * indicates mandatory questions.

Opinion on App for Social Media Content

Thank you for participating in this survey.

Note before you start:
We have included a question to monitor attention.
There are no right or wrong answers (except to the attention question), so please give your honest opinion.
In addition, please be aware that we will monitor and reject bot-generated answers, or answers that are completely unrelated to the question.
There are 19 questions in this survey

A note on privacy:
This survey is anonymous.
The record of your survey responses does not contain any identifying information about you, unless a specific survey question explicitly asked for it. If you used an identifying token to access this survey, please rest assured that this token will not be stored together with your responses. It is managed in a separate database and will only be updated to indicate whether you did (or did not) complete this survey. There is no way of matching identification tokens with survey responses.

Instructions

Please imagine the following scenario
—— [Privacy - Text condition] ——
There is a mobile app that can automatically analyze the texts you want to post on social media to protect your privacy.
The app works as follows:

- You can write the text that you want to post and the app will automatically analyze its content.
- If the app detects that the text contains information that could be private or sensitive, it shows a message and gives a suggestion.
- The app also highlights the most important parts that can be transformed.

—— [Non-privacy - Text condition] ——
There is a mobile app that can automatically analyze the texts you want to post on social media to enhance them for fun.
The app works as follows:

- You can write the text that you want to post and the app will automatically analyze its content.
- If the app detects that the text contains information that could be enhanced with emojis, it shows a message and gives a suggestion.
- The app also highlights the most important parts that can be transformed.

—— [Privacy - Image condition] ——
There is a mobile app that can automatically analyze the photos you want to post on social media to protect your privacy.
The app works as follows:

– You can upload the photo that you want to post and the the app will automatically analyze its content.
– If the app detects that the photo contains information that could be private or sensitive, it shows a message and gives a suggestion.
– The app also highlights the most important parts that can be transformed.

—— [Non-privacy - Image condition] ——
There is a mobile app that can automatically analyze the photos you want to post on social media to enhance them for fun.
The app works as follows:

– You can upload the photo that you want to post and the the app will automatically analyze its content.
– If the app detects that the photo contains information that could be enhanced with stickers, it shows a message and gives a suggestion.
– The app also highlights the most important parts that can be transformed.

—— [All conditions] ——
You can choose one of following options:

– Change the post to the suggestion
– Make changes manually: you can modify the suggestion, choose different transformation options, or change the post completely.
– Post without making any changes
– Cancel posting.

Other information about the app:

– The app is free.
– The app is a third party app, and not associated with a social media site.
– Use of the app is voluntary not obligatory.

Below is an example of how the app would work:
[Interface image corresponding to the condition]

Below are some examples of content and how the app would highlight it.
Please check them, imagining that you could post similar content about yourself or about people you know.
[5 examples of highlighted text or images, depending on the condition]

Q1. What was highlighted in example 3?*

Q2. Please indicate your agreement/disagreement with the following statements:*
• I would use this app in my daily life.
• I would recommend this app to people I know.
• I can think of people I know who would use this app.
• Using the app would get annoying.
• The app's automatic suggestion is satisfying.

– Strongly disagree
– Disagree
– Somewhat disagree
– Neither
– Somewhat agree
– Agree
– Strongly agree

Q3. Please explain your reasons for agreeing/disagreeing to the previous questions about the app. (open-ended)

Next, we will ask you some questions regarding privacy concerns that you may have about the app introduced in this survey.

Q4. Please indicate your agreement/disagreement with the following statements about the app introduced in this survey:*
• I believe that the location of my mobile device would be monitored at least part of the time by the app.
• I am concerned that the app could be collecting too much information about me.
• I am concerned that the app could monitor my activities on my mobile device.

– Strongly disagree
– Disagree
– Somewhat disagree
– Neither
– Somewhat agree
– Agree
– Strongly agree

Q5. Please indicate your agreement/disagreement with the following statements about the app introduced in this survey:*
• I feel that as a result of my using the app, others would know about me more than I am comfortable with.
• I believe that as a result of my using the app, information about me that I consider private would be more readily available to others than I would want.

• I feel that as a result of my using the app, information about me would be out there that, if used, will invade my privacy.

– Strongly disagree
– Disagree
– Somewhat disagree
– Neither
– Somewhat agree
– Agree
– Strongly agree

Q6. Please indicate your agreement/disagreement with the following statements about the app introduced in this survey:*
• I am concerned that the app could use my personal information for other purposes without notifying me or getting my authorization.
• When I give personal information to use the app, I am concerned that it could use my information for other purposes.
• I am concerned that the app could share my personal information with other entities without getting my authorization.

– Strongly disagree
– Disagree
– Somewhat disagree
– Neither
– Somewhat agree
– Agree
– Strongly agree

Q7. Please explain your reasons for agreeing/disagreeing to the previous questions on privacy concerns about the app.

Q8. Please write any other privacy concerns you have about the app.

Q9. Please indicate how much would the following privacy assurances and/or provider would reduce your privacy concerns about the app introduced in this survey.*
• The provider is a reputable for-profit company.
• The provider is a non-profit organization.
• The provider is an academic organization.
• The provider's privacy policy says that they will only use your data for improving the app.
• The app doesn't have ads.
• The provider's privacy policy says that they will not sell your data to third parties.
• The provider's privacy policy says that they follow laws and regulation for personal data protection.
• Your data is processed in your own mobile device, and not sent to the provider.
• Your data is processed so that it cannot be traced back to you.
• The provider explains how the app analyzes your content to detect and transform it.

– 1. Would not lower my privacy concerns at all
– 2
– 3
– 4
– 5
– 6
– 7. Would completely erase my privacy concerns

Q10. Please write any other assurance and/or any information that would reduce your privacy concerns.

Q11. Please indicate your agreement/disagreement with the following statements:*
• Compared to others, I am more sensitive about the way my personal information is handled.
• Keeping my information private is the most important thing to me.
• Compared to others, I tend to be more concerned about threats to my information privacy.

– Strongly disagree
– Disagree
– Somewhat disagree
– Neither
– Somewhat agree
– Agree
– Strongly agree

Q12. Please answer about your previous privacy experience:*
• How often have you personally experienced incidents whereby your personal information was used by some company or e-commerce web site without your authorization?
• How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?
• How often have you personally been the victim of what you felt was an improper invasion of privacy?

- Never
- Less than once in a month
- Once in a month
- Multiple times in a month
- Once in a week
- Multiple times in a week
- Once in a day
- Multiple times in a day

Q13. Please answer about your social media posting behavior:*
How often do you write a text post on social media?
How often do you post photos on social media?

- Never
- Very infrequently
- Infrequently
- Occasionally
- Sometimes
- Frequently
- Very frequently

Q14. Do you use or know a mobile app similar to the one introduced in this survey?*

- I have installed a similar app and use it frequently I have installed a similar app and use it frequently
- I have installed a similar app but I don't use it much I have installed a similar app but I don't use it much
- I know a similar app but I haven't installed it I know a similar app but I haven't installed it
- I don't know a similar app I don't know a similar app

Q15. Please write any other opinion or comment you wish to give about the app or the survey.

Demographics
Q16. Please indicate your age*

- 18 - 19
- 20 - 29
- 30 - 39
- 40 - 49
- 50 - 59
- 60 - 69
- 70 +

Q17. Please indicate your gender*

- Female
- Male
- Other (write-in)

Q18. Please enter your Amazon Mechanical Turk Worker ID*

Thank you for your participation.
Completion code: [generated code]
Please paste the code in the Amazon Mechanical Turk page.
Submit your survey.

Thank you for completing this survey.