A Comic-Based Approach to Permission Request Communication

Citation for published version:

Digital Object Identifier (DOI):
10.1016/j.cose.2022.102942

Link:
Link to publication record in Heriot-Watt Research Portal

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Computers and Security

Publisher Rights Statement:
© 2022 The Author(s).

General rights
Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
A comic-based approach to permission request communication

Katie Watson¹, Mike Just, Tessa Berg
Department of Computer Science, Heriot-Watt University, Edinburgh, Scotland, UK

A R T I C L E   I N F O
Article history:
Received 25 June 2022
Revised 14 September 2022
Accepted 30 September 2022
Available online 5 October 2022

Keywords:
Permission requests
Educational comics
Privacy

A B S T R A C T
Text-based permission requests do little to engage and inform smartphone users. Comics have recently been used with permission requests, though only in a survey of participants’ perceived reactions. In this paper we study more realistic reactions to comic-based and text-based permission requests. For our study, we invited participants to engage with a prototype version of a fictitious WebApp (PetConnect); participants were only informed of our intent to study permission requests at the end of the study. While using the app, participants were exposed to four permission request types (contact, storage, location and calendar) related to different functions of our app, using one of two styles of request (comic-based or text-based). Our results showed that participants were significantly more likely to deny the comic-based requests vs the text-based requests (47% vs 33%) and that comic-based requests were perceived to be more influential in participant decision making. Both styles of request were perceived to be equally relevant to the app, as well as equally annoying. We discuss several observations for future permission request design based on our participants’ explanations of their choices.

© 2022 The Author(s). Published by Elsevier Ltd.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

1. Introduction

Technology has become ever present in the daily lives of millions of people worldwide, with smartphone ownership and internet usage rising dramatically (Poushter, 2016). Many smartphone features are provided through applications (apps) that are designed to support users to carry out various tasks. To carry out these tasks apps typically require users to grant access to resources (e.g., location data) on their phone by responding to a permission request. However, these apps can sometimes endanger the smartphone user's privacy by the access given to resources and data (Bagrow et al., Feb. 2019; Blumenstock et al., Nov. 2015). As of March 2022, 96.7% of apps available on Android (Google Play) (Statista 2019) are free, and many use ad libraries (such as Admob) to generate an income. Dong et al. (2018) found that 2.5% of apps use Admob which violates the ad library policies by requesting more permissions than necessary to collect additional user data (Chin et al., 2012). Apps sometimes request access to resources that are not necessarily required (Dong et al., 2018), for example a location/mapping app that requests access to a phone's contacts. Even when the requested access might be necessary, the permission request descriptions may not be sufficiently informative or engaging, with users reporting their distracting nature (Felt et al., 2011; Harris et al., 2015; Kelley et al., 2012; Micallef et al., 2017; Westermann et al., 2015).

Previous studies have found that users typically pay little attention to the currently employed, text-based permission requests, and they display low comprehension of what is being asked of them (Felt et al., 2012). Researchers have concluded that users are generally unaware of data collection practices via smartphone apps and are not comfortable with the amount of data being gathered, and with whom this data is being shared (Almuhamedi et al., 2015; Balebako et al., 2013). This suggests that the current medium of text-based permission requests may not adequately inform users, and the requests can leave some smartphone users unaware of the potential risks to the privacy of their data.

In this paper we investigate the viability of two styles of permission requests and highlight the influence these requests can have on users. To this end, we report on the impact and reception of comic-based and text-based permission requests. For our study, 98 participants interacted with a fictitious WebApp that we created (PetConnect), from which we collected their responses to the in-app permission requests (allow or deny) and their reasons in an online survey. We sought more realistic reactions than previous work (Watson et al., 2020) so that as our participants were unaware of the privacy focus of the study till after their interaction with our WebApp. This allowed us to investigate the permission requests in a more realistic setting than has been done before, and further understand the impact of alternative permission requests. Our approach centres on two research questions:

https://doi.org/10.1016/j.cose.2022.102942
0167-4048/© 2022 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)
RQ1: Will participant responses (allow or deny) to the two styles of permission requests differ?

RQ2: Will participant reasons for their responses (allow or deny) differ between the two styles of permission requests?

In Section 2 we discuss related work, followed by a review of our methodology in Section 3. In Section 4 we present our results, and in Section 5 we respond to our research questions and consider the implications for future permission request designs. In Section 6 we highlight some study limitations, followed by our conclusions and future work in Section 7.

2. Related work

Current measures to protect and inform users are often filled with complicated jargon (Kelley et al., 2009; Talib et al., 2014) and may leave users unaware of the risks to their privacy (Balebako et al., 2013; Malandrino et al., 2013; Mylonas et al., 2013). Legislative protections mean that app providers are required to gain informed consent from users to collect and use personal data. However, these measures are often overlooked (Kelley et al., 2013), not comprehensive or not fully understood by users (Talib et al., 2014; King et al., 2011). Once access has been granted to some smartphone resources, data collection can begin, and even though access can be revoked, the data that has been previously collected is still retained (unless a user specifically requests it to be deleted). Research has shown that behaviours towards the protection of some information can change over time (Sadegh et al., 2009). Users should be able to change their mind and be made aware of the ramifications to their data when deciding whether to allow or deny a request. The introduction of Ask on First Use (AOFU) permission requests, or runtime permissions does somewhat negate this, as access is not granted until required. However, researchers (Shen et al. 2021) found that only a small percentage of users (6.1%) could accurately infer the scope of AOFU based off the system, which indicates that the information provided may not be sufficient.

Alongside this, there are also permissions within the Other category that are automatically accepted through the installation process. This category contains all the capabilities the user is allowing by downloading, or leaving a pre-installed app enabled on their device, such as: have full network access, and prevent phone from sleeping.

2.1. Previous permission request improvements

Researchers have previously investigated ways to simplify privacy-related agreements (such as privacy policies, Terms & Conditions (T&C), and permission requests) using various techniques, e.g., using standardized language (Gideon et al., 2006), summary reports (Good et al., 2005) and privacy policies (Gluck et al., 2016; Kay and Terry, 2010). While these methods were found to be more inviting for readers, the improvements did not necessarily lead to better comprehension of the actual policies (McDonald et al., 2009).

Further research has investigated how personalisation and contextualisation can affect user receptiveness to permission requests. Tan et al. (2014) found that participants were more likely to grant access to permission requests which contained an explanation of why the app needed access, regardless of whether the explanation contained useful information. Despite this, some of the personalised requests were questionable for widespread use. Related to permission requests, Aimeur et al. (2016) similarly found that including additional information in privacy policies, and allowing participants to personalise them made companies appear more trustworthy to the participants which in turn could make them more likely to grant requests. Raji et al. (2011) also demonstrated the importance of personalisation, as they discovered that participants did not understand the “sensitive nature” of the data shown if they felt they had little or no personal stake in it. Personalisation could be used to emphasise their stake in the matter, with the personalisation being as simple as “Company X now know where you live” or “100, 000 people have access to the location of your home, friends and work place”. Harbach et al. (2014) found that users made more privacy conscious decisions when installing apps when presented with personalised demonstrations of the consequences that granting access could have. These studies suggest that personalisation can make companies appear more trustworthy to users and as such should be implemented carefully to avoid the illusion of control or trust in a company that might compromise user privacy (Benson et al., 2015).

Contextualisation refers to information that is concerned with the circumstances surrounding the user. Several studies have examined how the framing of privacy information can influence user response. Research conducted by Shih et al. (2015) found that participants were more willing to disclose their data when no purpose was specified, and when some specific purposes were shown. Participants were also found to be influenced by type of purpose, sharing the least when the data access was exclusively beneficial to the developers. Socially framed information, such as “91% of people share location” has also been linked to increased sharing of personal information (Zhang and Xu, 2016), which suggests care should be taken to keep misinterpretation of the risks to a minimum. Taken together, these findings suggest that there is a role for alternative means of communicating privacy-related information, such as comics, to help frame information provided within permission requests, to better engage users, and allow them to make more informed decisions.

2.2. Communication with comics

The unique composition of comics, in which a narrative is conveyed through a series of images accompanied by text, is what has captured and held readers attention throughout the years (McCloud, 1994; Waugh, 1991). Päivio argues that as pictures are processed in two areas of the brain (visual and verbal), this results in a higher retention and recollection of images than words (Päivio, 1973). Comics have proven to be effective educational tools, with research showing their successful implementation in multiple fields, including healthcare and education (Delp and Jones, 1996, Reumont and Alexandra, 2020, Tekle-Haimanot et al, 2016).

Comics have proven similarly effective in online security and privacy contexts (Mekhail et al., 2014, Sikoryak, 2015, Tabassum et al., 2018, Zhang-Kennedy et al., 2017a). Comics have been used to reiterate Terms and Conditions (T&C), Sikoryak created a rendition of Apple’s T&C, with each page an adaption of classic comic artists (Sikoryak, 2015). Tabassum et al. (2018) also explored the use of a comic version of T&C as a replacement for traditional text. They found that comics held user attention for longer, but did not improve comprehension (they indicated this result may have been caused by the small sample size of participants). Zhang-Kennedy et al. (2017a), Zhang-Kennedy et al. (2016) found that the graphical and interactive elements of their comics (Secure Comics) aided reader comprehension of the information presented. Additionally, they found that user understanding of security threats had improved, and when facilitated, readers made more security conscious decisions. Zhang-Kennedy and Chiasson additionally used an online, interactive comic to teach users about smartphone location data (Zhang-Kennedy and Chiasson, 2014). Significant improvements in their participants’ understanding were reported, with 53% of participants changing their location-based settings. In a similar vein, Mekhail et al. (2014) explored the use of infographics in a mo-
bile privacy context to determine whether they were more beneficial for users than text. They found the infographic information led to 64% of participants reportedly taking additional measures to protect their privacy, and approximately two thirds of the users could describe the concepts shown. All the above studies were conducted on large screens or on print outs, which are different mediums to smartphones. Thus, while the majority of these studies show promise, the results may not transfer. However, not all comic research in privacy has met with success. Anaraky et al. (2019) tested their privacy policy comics inspired by Knijnenburg and Cherry (2016) 2016 hypothesis, and found that the participants who received comics reported lower self-efficacy, and ease of use. Though, the comics displayed to participants made heavy use of narrative text, stylized screenshots and were quite busy in appearance. There has only been one investigation on the use of comics for permission requests: Watson et al. (2020). Their investigation found that 52% of participants preferred the comic-based requests, and 87.3% stated they felt that the comic-based permission requests were somewhat or extremely easy to understand. However, theirs was a study that asked participants to anticipate their reactions to static comic-based and text-based permission request images, and participants were aware of the privacy nature of the study, so that the performance of the participants might not necessarily reflect realistic behaviour.

3. Methodology

To assess our permission requests in a more realistic setting, we created a fictitious web application (WebApp) called PetConnect that we asked our participants to use and evaluate. PetConnect was designed to allow participants to connect with other pet owners and look after their pets. As part of the set-up of PetConnect, participants were shown several ask-on-first-use (AOFU) permission requests. Participants were asked to use a smartphone or tablet to take part and were informed that the study was focused on the experience of the WebApp - they were not aware that it was a study on app privacy permission requests (though they were debriefed on this aspect at the end of the study). The study was approved by the ethics review board at the authors' institution, and it consisted of 3 stages, (1) demographics and introduction survey (2) use of the WebApp, and (3) a survey covering questions about the permission requests. We discuss these stages in Section 3.2, after first presenting our permission request design.

3.1. Permission request design

We used two styles of permission requests for the study: a comic-based style and a text-based style. The comic-based permission requests were based on the designs of Watson et al. (2020). The text-based permission requests were based on the typical permission request style used on today’s smartphones, with the addition of some additional text to provide content similar to the comic-based requests. For each style of permission request we designed four types of requests based on common requests for permission on today’s smartphones; contact, storage, location and calendar (Harris and Chin, 2016). We used two conditions in our study: participants in the first condition only saw the comic-based requests and participants in the second condition only saw text-based requests. Fig. 1 provides an example of the two styles of permission requests used for a location request.

![Fig. 1. Comic-based (left) and text-based permission request (right) for the location permission.](image-url)
The comics included attributes that were intended to increase user engagement and awareness, based on previous research into comic design (Zhang-Kennedy et al., 2016). This included a focus on humour, characters, narrative, and aesthetics. Two main characters (human and cat) were designed for the comics; they encounter permission requests and consider the impact. The use of narrative and characters in this format was designed to guide the users towards understanding of the complexity behind permission requests and bring awareness to the different types of data collection (Watson et al., 2020; Zhang-Kennedy et al., 2016; Lewis, 1989).

### 3.2. WebApp and questionnaire

In the first stage, participants were presented with an overview of the study (experience of using PetConnect). If consent was provided, demographic information was then collected (gender, age, current country of residence, and mobile device used). Each participant was then directed to the PetConnect WebApp for stage 2 of the study.

In the second stage, we employed a between-subjects approach with two conditions, one for each style of permission request. At the end of stage 1, participants were redirected to the WebApp that would display either comic-based or text-based permission requests, which alternated when each new participant entered the WebApp.

Upon visiting the WebApp, participants were asked to follow a series of steps to complete an example user journey. These steps included (1) signing up to the service and choosing which type of pet they are interested in, (2) the option to invite their friends to the app, (3) the choice to upload a profile picture (4) setting their location to find pets in their area, and (5) viewing pet profiles and scheduling an event. In total, there were four permission request types presented to participants (either in text or comic form): contacts, storage, calendar, and location. Fig. 2 shows the progression of steps, including the permission request types.

The contact, storage, and calendar permission types could be skipped by participants, as their actions did not lead to the request being prompted. Participants could choose to not to share with friends (contacts), not to upload a profile picture (storage), or to sign-out of the WebApp early, before scheduling an event (thereby skipping the calendar permission). However, all participants were asked if they would like to allow the location permission request, though users had the option to deny the location permission request and manually type in their location. Each permission type was requested alongside a corresponding action in the WebApp (following the AOFU permission reactions). Fig. 3 shows a preview of the WebApp pet profile page (for a full preview see appendices. For each of the permission requests participants were required to choose to allow or deny the request, and they could also click “learn more” to discover further information about the request. None of the permission requests were required to be allowed for the app to function properly. Participant responses (allow or deny) were recorded. To see this journey see Appendices.

In the third stage, participants were taken to a final survey where they were asked one question about their overall experience with the WebApp, and then a series of questions related to the permission requests, including whether they remembered seeing any permission requests (and if so, which ones), why they allowed/denied the permission requests, followed by three questions related to participants’ overall perceptions of the permission requests (answered on a 5-point Likert scale, i.e., “I strongly agree, I agree, I neither agree or disagree, I disagree, I strongly disagree”).

(1) Do you feel the information included in the permission requests influenced your response? (2) How relevant (if at all) did you find the permission requests? (3) How annoying did you find the permission requests you were shown?

Participants were also asked if they wanted to provide further information to explain their responses. As a final question, we asked participants whether they had any suggestions for improving the permission requests. To conclude, participants were debriefed about their experience and told that the true focus of the survey was on permission requests. Participants were also given the chance to enter a prize draw for one of five £20 Amazon Vouchers for their participation.

### 3.3. Analysis approach

The survey and WebApp results were analysed using a combination of parametric (Chi-squared test) and non-parametric statistical (Wilcoxon Signed-Rank, Mann-Whitney U) tests. All the statistically significant results are reported, alongside some of the interesting non-significant results. Due to multiple comparisons being made Bonferroni Corrections were employed, dividing the significance value by the number of tests run (8).

The qualitative results from the survey, where participants were asked to explain their choices, were analysed using Content Analysis. This consisted of the researcher familiarizing themselves with the data, highlighting phrases from the text to capture key concepts, coding the data, identifying themes across the coded data, then refining these themes and writing up results. In order to check the reliability of the content analysis a Krippendorff’s alpha (Hayes and Krippendorff, 2007) inter-coder reliability test was run with one other independent coder (who was not involved in our study). A sample was randomly selected, and alongside generated codes was sent to the second coder. The chosen sample was approximately 10% (40 units) of the data gathered, for each of the two conditions (Lombard et al., 2010). Results showed a solid inter-coder reliability score $\alpha = 0.8203$.

### 4. Results

Both qualitative and quantitative data were collected and results on each are presented. Participants were assigned a random
6-digit number at the beginning of the survey, that we used to link their survey responses to their use of the WebApp. Below, participants are assigned shorter identifiers (P1-P98) and matched to participant quotations.

4.1. Participant details

To be included in the study participants had to be 18 years of age or older, understand the English language, and own a smartphone or tablet. A total of 206 participants were recruited through social media (including Twitter and LinkedIn), and snowball sampling. Of the 206, 109 participants completed the three stages of the study and 98 did so using a smartphone or tablet. We present our results for these 98 participants, of which 40 were shown text-based permission requests and 58 were shown comic-based permission requests. Out of the 98 responses, 46 used an Android smartphone, 46 an iOS smartphone, and 6 a tablet (3 iPads, 1 MacBook Air, 2 Samsung tablets). Participant ages ranged from 18 to 65, with a mean age of 32 years. Additionally, 33 identified as male and 64 identified as female and 1 preferred not to say. The majority were from the United Kingdom (58%), followed by New Zealand (20%), United States of America (5%) and then a combination from 11 other countries. In terms of employment, most participants were employed (62%) or students (34%). Participants were asked to pick more than one response for employment status, and 7 participants chose to do so. Participants were also able to take part in the study whenever and from wherever suited them best.

4.2. Responses to permission request styles (Quantitative findings)

All 98 participants were presented with the location permission request (40 text and 58 comic), while 86 experienced the calendar permission (37 text and 49 comic), 26 the storage permission (10 text and 16 comic), and 9 the contacts permission (5 text and 4 comic). In total, the comic permission requests were experienced 128 times and the text 92 times. A Wilcoxon Signed Rank test revealed that participants shown the comic-based requests were significantly more likely to deny a permission request than those shown the text-based versions. Overall, when including permissions which were unseen, 25.8% of participants denied the comic-based requests, whereas 18.8% denied text. \( Z = -12.804, p \geq 0.00 \). When separated into each permission type, Chi-Squared tests revealed that this difference is only statistically significant for the location permission request, \( \chi^2 = 4.106, p = 0.045 \) (results can be seen in Table 1). However, it is important to note that the number of participants exposed to each permission request type varied. The “learn more” button was largely ignored, with only 7 instances of use, and 6 participants selecting it: contacts (2) storage (2) and location (3). Due to multiple comparisons being made, Bonferroni Corrections (Cabin and Mitchell, 2000) were employed, dividing the significance value by the number of tests run \((0.5/4 = 0.125)\).

In stage 3, after using the WebApp, participants were asked if they remembered experiencing any permission requests, and if so to provide the names (types) of the requests that they remembered. Only 11 participants indicated that they did not remember any requests (2 text, 9 comic), while the remaining participants (38 text, 49 comic) correctly responded with at least some of the permission request types that they had experienced. Of those who said that they remembered experiencing the permission requests, 55% (22) who were shown the text-based permission requests correctly responded with all the permission request types that they were exposed to, compared to 51.7% (30) of the comic-based participants. This difference was not statistically significant, \( \chi^2 = 0.451, p = 0.068 \). There was no significant difference when comparing each of the permission request types separately.

To analyse whether either of the permission request styles influenced a participants’ decision to allow or deny the request,
a Mann-Whitney U test revealed that participants who were shown the comic-based permissions felt they were more influential \( U = 697.5, p = 0.013 \), compared to those shown the text-based requests. The answer “probably yes” was selected by 35% of those shown comic and 7.8% for text, and “definitely yes” with 17.5% comic, and 2% text. This difference was also found to be significant for women, but not for men (women – U = 248, \( p = 0.014 \), men – U = 98.5, \( p = 0.524 \)).

There was no significant difference between the comic-based and text-based request styles for the perceived level of annoyance of the permission requests. Overall, most participants found the requests to be annoying, with the majority in both request styles reporting them to be very annoying (21.6% comic, 27.5% text) or extremely annoying (35% text and 29.4% comic). Finally, there was no significant difference between the two request styles, for the perceived relevance of the requests (e.g., in terms of supporting the app functionality), with most users finding the requests either “somewhat relevant” (43.1% comic, 35% text) or “extremely relevant” (32.8% comic, 40% text).

Participant’s response time was also recorded. An Independent T-test found that users who used the text-based requests spent significantly less time on average (3.56 s) viewing the request, than those who were shown the comic-based versions (8.15 s). \( (t(97)) = -4.882, p < 0.000 \).

A significant difference was found in the location and calendar permission requests. Participants spent the least amount of time on the location text-based permission (2.93 s) and most on the storage comic-based permission (11.88). The average number of words (excluding the header) on the text-based permissions was 13.5 words, whereas the comic permissions included an average of 18.5 words.

4.3. Perceptions of permission request styles (Qualitative findings)

In stage 3, participants were asked about their perception of the permission request style that they used in terms of reasons related to their allow/deny responses. Around two thirds of participants provided at least some responses to describe their perceptions. The presentation of the codes below shows the number of coded statements that were associated with each request style in parenthesis after the permission style (i.e., text (15)).

Participants largely reported that they chose to allow the permission requests for the functionality of the WebApp, (text (15), comic (17) e.g., “To find pets near me and for me to be able to schedule an event” (P24 text). Also, participants from both request styles felt that some of the permission requests were necessary for the app to function e.g., “Allowed because appeared required” (P11 text), “It seemed necessary to be able to complete the process. The short comic summarised the permission request in an interesting way” (P70 comic). Some participants expanded on this further, “usually apps don’t work if you don’t allow what they ask for” (P40 text). Similarly, participants also commented that they felt the requests were imposed upon them and were required to continue app use e.g., “I didn’t grant those I felt were unnecessary (contacts and storage or camera) and granted those that were necessary to use the app” (P65 comic). A few participants who used the comic-based requests also indicated their acceptance was out of habit, as many apps require access for the user to continue:

“It gave me a greater awareness of handing over my data but as these pop so frequently when using apps website etc I have developed a tendency to accept them as many sites will not let you continue to the page if you do not comply” (P48 comic).

A few participants from both request styles also mentioned the convenience that permissions offer (text (3), comic (4)) as they accepted the permission request to make their life easier: “I need to know information around me. Locating myself is a reasonable and convenient way” (P84 text). Whereas some participants reported not being bothered by the requests and taking the path of least resistance, at times with no logical reason as to why e.g., “Storage to upload a photo, location to be able to see what pets were available in my area, calendar not actually sure why” (P22 comic).

Furthermore, participants from both request styles also stated that for some permission types they felt that little to no sensitive personal information could be collected through allowing access. However, this comfort was often restricted to one permission type: “I allowed media and calendar access as I feel they aren’t invasive. I disallowed Location as, like the cartoon said, I could be tracked later without my consent” (P90 comic).

In terms of reasons for denying permission request, participants from both request styles expressed uncertainty towards some of the permission types requested by the app, as participants reported that they felt that some or all the permission requests were irrelevant or unnecessary (text (5), comic (9)):

“I didn’t allow contacts and calendar as I don’t feel these are needed. I did do camera as I wanted to upload an image and location to find pets in my area” (P33 text), and

“Hard to say, they were very clear about what they wanted. It wasn’t confusing at all. But I think what they wanted was inappropriate. I would just not use the app if those requests were required” (P60 comic).

However, it was reported in both request styles that due to conceived pressure the participant chose to accept the request anyway:

“I was a bit sceptical to sharing my location on an unknown app, although i did. And did not want to share a profile picture” (P38 text).

Participants who used the comic-based permission requests (6) commented that the additional information in the comic requests changed their typical behaviour to reflect a more privacy conscious approach, as it made them think twice about their responses to the permission requests:

“I feel like normally I would accept, however given the cartoon explanation of what can actually be access by the app I reconsidered and pressed deny” (P3 comic), and

| Table 1 |
| --- | --- | --- | --- |
| Table Head | N | Allowed Frequency | Percent |
| Contact | Text | 5 | 2 | 40% |
| Comic | 4 | 1 | 25% |
| Storage | Text | 10 | 5 | 50% |
| Comic | 16 | 7 | 43.8% |
| Location | Text | 40 | 30 | 75% |
| Comic | 58 | 32 | 55.2% |
| Calendar | Text | 37 | 25 | 67.6% |
| Comic | 49 | 28 | 57.1% |

Formula:

\( x^2 = 0.228 \)

\( p = 0.635 \)

\( x^2 = 0.097 \)

\( p = 0.756 \)

\( x^2 = 4.106 \)

\( p = 0.045 \)

\( x^2 = 0.976 \)

\( p = 0.325 \)

Computers & Security 124 (2022) 102942

K. Watson, M. Just and T. Berg
“The comic strips really made me think. I might have been tempted to just accept the permission request to make it easier to complete the task, but then I could see that I was sending too much” (P57 comic).

One participant who used the comic-based requests expressed regret about their choices after reflection, during the survey stage of our investigation, as they questioned whether the permissions requested were necessary.

“The contacts permission seemed irrelevant, as did the GPS location (wouldn’t an address or approximate location suffice?). The calendar permission could have probably been replaced with setting certain availability timeslots. I regret my choices now...” (P2 comic).

Privacy conscious reasons were the main cause stated by participants for having denied both styles of requests (text (6), comic (24)), though note that there were more participants who were exposed to the comic-based requests. Also, some participants (text (2), comic (4)) wrote that they always denied all, or some specific permission request types (e.g., location) regardless of the app, due to privacy concerns or out of habit, e.g., “denied all of them, since I do not think this app, even it is great, should have such wide access to data on my phone” (P55 text). Additionally, due to the supplementary information provided in both styles of permission requests, both request styles had participants who commented that the permission request made them feel nervous or scared about their personal data, and what could be collected. “It was scary to share too much info on an unknown app” (P38 comic).

The participants’ perception of the permission requests showed that the additional information provided an important influence for their response, for both allowing or denying permission requests. Participants (text (4)) of those who were exposed to the text-based permissions stated that the extra information was useful, with participants (text (3)), stating they found the information clear. This went both ways with one accepting: “It showed the reason, which I accepted” (P64 text), and another becoming more privacy conscious: “They explained what they would access by you accepting or denying the permission request” (P45 text). Further, those who used the comic-based permissions commented upon an increase in awareness and understanding (comic (14)) and participants indicated they felt the information was displayed in a clear manner (comic (7)):

“I often forget what exactly enabling location services does and the cartoon quickly reminded me about what it means and got me thinking about whether it actually is necessary in this situation” (P14 comic), and

“It exposing why the permission was being requested and what was going to happen to the data” (P75 comic).

Participants further commented that the comic-based permission requests were an engaging medium and that the visuals of the comics improved their experience (comic (111)): “I don’t know how something so simple could be improved” (P66 comic). Other participants (comic (2)) said that they felt the personalisation of the comics helped enhance their experience and enjoyment of the permission requests, e.g., “Liked the inclusion of the pet I was choosing, and the cartoon raised my awareness of what access involved” (P7 comic). However, one other participant commented that they already understood the implications: “already have preconceived notions about the requested permissions” (P37 comic).

When participants were asked how relevant they felt the permission requests were, participants (text (8) comic (11)) said that they understood the reason for some of the permission requests. One participant also theorised this could be because this level of access is standard for most apps available in today’s market e.g., “They are standard permissions for most websites/apps. The location one was more relevant than the calendar permission as I had to manually select dates anyway” (P46 text). When asked how they felt the permission request style impacted their decision, participants (text (2), comic (5)), stated that they felt the permission request style had no impact on their decision to allow or deny. However, one participant who used the comic-based permissions reported confusion, and expressed a lack in trust caused by the comics in the permission requests:

“I found them a little confusing it made it seem like it didn’t want me to give them access, which is odd when they [the website] were asking for my contact initially? They reduced how much I trusted this website asking in the first place” (P58 comic).

The trustworthiness of the WebApp itself was also highlighted by participants from both conditions (text (2), comic (1)), who found the WebApp friendly, e.g., “Allowed all because it looked friendly” (P68 text).

It is also important to note that a small number of participants (text (2), comic (2)), cited that their responses to the permission requests were influenced by the knowledge that they were participating in a study. This included participants who accepted or denied all or some of the permission types.

4.4. Design feedback

All participants from both conditions were divided about whether the requests needed additional improvement, with about one-third expressing each of “yes” and “no” and “unsure”, with no significant difference between the conditions.

Participants from both conditions cited that more information should be included within the permission requests (text (7), comic (11)). This included why the data was being collected and how the data collected will be used: “More info on why and how I could subsequently control it” (P54 text), and “Give a reason why its required/what is done with the data” (P32 comic). A few participants also inquired about data being sent to third parties, and how that effects the any control they have:

“It could explain exactly why the request is needed, what data will be taken, how it’s stored, if it’s passed to any third-parties and my options to request deletion. Also - if I delete, then does my data get deleted on third party too?” (P3 comic).

Additionally, participants (text (1) comic (6)) indicated that it should be clearer if the permission request is required in order for the app to function. One participant who was exposed to the comic-based style stated that if they were aware that data could be input manually (such as entering their location), they would have denied all permissions: “Made clearer if they were vital to the functionality of the app. If data could be input manually and I was aware of this I would have denied all permissions.” (P49 comic).

As well as this, participants from both styles (text (3), comic (1)) recommended having all the permission requests to be asked at once. Participants suggested this could occur at the beginning of the app interactions, to reduce interruption, as the AOFU felt like a barrier to completing certain tasks e.g.,

“It would have been nice to get the requests up-front at the beginning of the process - each step of finding a pet and booking time with the owner was interrupted by permission requests, and it was super jarring. Would have been niceer to get them all out of the way up front with some context on why each is needed, so that I could have a simple experience afterwards” (P6 text).

Alongside this, one participant from each condition suggested including an option where the permission is turned off when not using the app, e.g., “I know they’re necessary, maybe done options around how to turn them off when not using the app?” (P69 text).

Participants from both conditions indicated that they felt apps should not be asking for inappropriate permissions, with participants also stating they felt sharing to third parties was unsuitable:
“I think the location is not suitable as this can be discussed privately and confidentially with the pet owner themselves without giving access to third parties or unsecure connections” (P91 text).

The appearance of both permission requests styles was also commented on, with one participant who was exposed to the text-based permission requests, suggesting a change to the colour of the buttons (allow and deny) to see if it primes a different response, e.g., “You could change the colour of the buttons and see if it primes a different sort of response” (P83 text). For the comic-based permissions participants (4) suggested the addition of colour to the comics to help them “stand out more” (P90 comic).

5. Discussion

The results highlight the impact the two styles of permission requests had over the participants. The discussion will be split into the two research questions set for this investigation and the design implications suggested by the participants.

5.1. RQ1: will participants responses (allow or deny) to the two styles of permission requests differ?

The results suggest that the style of permission requests did play a role in how participants responded. Significantly more participants (47% comic vs 33% text) chose to deny the comic-based permission. Qualitative results suggest that participants through the comic-based permission requests were either reminded or informed of privacy implications which resulted in them declining the request. This apparent increase in privacy conscious behaviour has been similarly seen in previous work where users, once made aware of potential data collection including frequency of collection, displayed a more privacy conscious response (Balebako et al., 2013; Watson et al., 2020; Zhang-Kennedy and Chiasson, 2014; Wijesekera et al., 2018). As both styles contained additional information this suggests that the comic-based style was more effective at increasing privacy conscious behaviour. However, most of the permission requests were allowed (67% text, 53% comic), with many participants indicating they thought this was due to the functionality required for the app. Despite this, the results suggest that while text-based permission requests containing additional information may give users pause for thought, comic-based permission requests are even less likely to be granted. Potential reasons as to why participants allowed or declined the requests are discussed in response to RQ2 below.

5.2. RQ2: will participants reasons for their responses (allow or deny) differ between the two styles of permission requests?

Participants of both styles of permission requests felt that certain and in some cases all, types of requests were necessary or required for the app to function. The fact that participants largely reported that they felt that some or all the permission requests were mandatory has potentially resulted in the acceptance of permissions out of habit or convenience. As users wanted to use an app to accomplish some purpose so they do not want to be faced with an app where some functionalities did not work potentially having to go back and to allow a permission to gain access to the functionality. Previous research has also highlighted how users are becoming desensitized to permission requests (Harris et al., 2015) as nothing bad has happened to them or their data that they are aware of. This lack of understanding of permission requests benefits the developers, as users could be unnecessarily allowing access to personal data.

Results indicate that when participants from both request styles perceive the risks to their data through the additional information, or when they felt that the permission request type (e.g., contacts) was inappropriate, they are willing to take measures to protect their privacy, similar to results seen by Mekhail et al. (2014). Comic-based requests were statistically more likely to be denied. This result suggests that the comic style of permission request had a greater influence over participants. Qualitative results from participants suggest that this is due to the increased awareness and understanding offered by the comics. Zhang-Kennedy’s work on secure comics identified similar effects, though related to participants’ understanding of privacy risks (Zhang-Kennedy et al., 2016; Zhang-Kennedy et al., 2017b). This theory is supported by multiple participants who used the comic-based requests, reporting that they reassessed their decision as the information provided in the permission requests highlighted the dangers of data collection. This is similar to findings from Shih et al. (2015) who found users were less likely to share data when the access was exclusively beneficial to the developers. Some participants in our investigation were found to accept permission requests due to feelings of obligations and some have shown regret accepting certain permission requests. This indicates that some users may not be comfortable with the access they are allowing but perhaps feel obligated to allow these permissions.

The additional information, presented in comic form, was found to be more engaging to participants, with some reporting that the medium of comics offers some personalisation. The personalisation could be achieved through the characters displayed within the comics. One participant remarked on the parallels between themselves and the main character, in that they were looking for a cat and the character in the comics had a cat. This similarity could have contributed to the formation of a connection to the main character and in turn made the participant more likely to deny the permission requests. This concept has been seen in previous research, with Hoffner and Buchanan (2005) investigation which focused on young adults. It found that people displayed a wishful identification (the desire to be like or to mimic) with same gendered characters. Additionally, if the participants did relate to the human character and felt a sense of personalisation when shown alongside the character, some of the consequences could result in more privacy conscious decisions. Authors such as Mylonas et al. (2013) have found in their work that users made more privacy conscious decisions when installing apps when presented with personalised demonstrations of the consequences of allowing access.

The trustworthiness of the WebApp was also commented on by a few participants, who reported that the app itself influenced their response. This phenomenon has also been found in research, with Harris et al. (2015) investigation which discovered that 63% of their participants felt there was often a good reason for apps to request questionable permissions and trusted the Apple App Store and Google Play markets.

5.3. Design implications

The most suggested means of improvement for both comic and text-based permission requests was the addition of more information. This includes why the permission is requested, if it is required for the functionality of the app, what control users have over their data, and what is done with the data collected. This was similarly found in the investigation run by Watson et al. (2020).

However, the inclusion of information about the reasons for allowing a permission, could prove problematic. The app providers could claim permissions improve the functionality or convenience of an app, while their main purpose of data collection is to make a profit through targeted advertisements. If not monitored, the framing of information could encourage unnecessary approval of certain permissions. For example, providers may leave out some reasons for data collection by the app, when the manual input of data
(such as entering a location) would suffice. This is seen in research by Aimeur et al. (2016) were the addition of supplementary information resulted in participants making less privacy conscious decisions. App providers have a duty to their users to inform users of what data will be collected, how it will be collected, why it will be collected, and how it will be used. Comic-based permission requests are able to convey information to users more effectively than solely text-based permission requests and likely would be more favourable to providers than making privacy policies more accessible and understandable. App stores should and could implement and encourage the use of comic-based permission requests as a proactive measure to protect the privacy of users and ensure app providers present a similar narrative.

Research has shown that data leakage can occur though data collection (Balebako et al., 2013; Malandrino et al., 2013), and that a request for data deletion by the supplier is often not successful (McMillan et al., 2010). The participants suggestion of more information concerning the control of their data is problematic, as a greater understanding and awareness of the control has been linked to an increase in disclosure of personal information (Aimeur et al., 2016; Benson et al., 2015). This is also seen in the results for the online survey run in Watson et al. (2020) work, where the inclusion of solutions reminded users that they could change their mind later. This resulted in less privacy conscious behaviour. Furthermore, if the control, such as the complete deletion of data cannot be carried out successfully, e.g., the data has already been passed on. This negates the protection the user feels through this control, and they might not have allowed the request in the first place.

In addition to this, participants have expressed a desire for all the required permission requests to be handled on installation when they first open the app. This could reduce the annoyance felt by the interruptions caused by the AOFU permissions and could allow for the introduction of a new permission statement which discloses the functions carried out by the app that fall into the other category. Ideally this should be a request to allow access to the other category functions. AOFU permissions have been found to in accurately reflect users privacy preferences (Wijesekera et al., 2018). However, participants may be prone to ignore permissions if they were to appear in a similar manner to Terms and Conditions and notices (Jalib et al., 2014; Aslam, 2006).

It is also important to note, that during this investigation some participants raised the idea of including more information related to a permission request. The option for more information was included within the permission requests as a “learn more” button, which participants largely ignored (only used in 7 instances). This suggests that any inclusion of information would need to be within the request itself, or that participants like the idea of more information, but are not willing to look for themselves.

In terms of appearance, the comic-based requests received more feedback, for example, participants suggested the addition of colour. This addition could be explored in future work. However, colour can be problematic due to different cultural colour associations Aslam (2006) and can make the comic busy and unclear. For the content of both styles of permission requests, personalisation and how it effects user response could be further explored, as previous research has shown that how the way information is framed can affect user behaviour (Raj et al., 2011; Zhang and Xu, 2016).

6. Limitations

Since comic-based permission requests are a novelty compared to the traditional text-based permission requests, it is possible that participant responses may change based on the reduction of novelty value of the comics. Additionally, the WebApp required access to a browser on the participants device, which may have altered the user’s perception of the permission requests asked. Even though participants did not initially know that they were taking part in a permission request study, they were aware that they were taking part in some study, which may have led to less realistic responses by participants. Participants who took part were all recruited online. Recruitment for the studies was largely done through Social Media sites. This could mean that the participants may have an above average level of technological skill and familiarity with smartphones. Lastly, the survey was not limited to users on smartphones. Therefore, the effectiveness of the comic-based permission requests may vary between participants using a larger screen where the user experience is different.

7. Conclusion and future work

The results of our investigation suggest that further work is required into permission requests styles and the comic style is one example of a potentially viable medium. Participants are more likely to react differently to permission requests when they have an increased awareness of the privacy implications. This behaviour was more apparent in those presented with comic-based requests; however, it was also present for those shown the text-based requests. Many participants reported allowing requests because they believed the request was required for the functionality of the app. Those shown comic-based permission requests questioned the relevance of the permission requests and were less likely to allow them.

Future work could explore this further with “in the wild”, longitudinal studies with fully functioning apps to assess more realistic behaviours. It could also explore additional variations of comic and text-based permission requests (e.g., different art styles which could be culturally influenced and the addition of colour). The personalisation of permission requests is another avenue of research that could provide rich results. This could allow for a heavier focus on the role certain characters play in influence, and of further personalisation of the side character, such as the reader being able to choose the type of animal companion. Another avenue which could be explored is participants perception and potential desire to learn about the other category of permission requests. Specifically, whether apps should disclose them more publicly, or if they should be a required permission request to use or have a pre-installed app enabled.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Acknowledgments

We would like to thank all the participants who took part in the study, and Laura Watson and Peter McCready who helped construct the Web app.
Appendices
K. Watson, M. Just and T. Berg


Katie Watson currently works as a user researcher and has completed her PhD titled “Novel, Comic-Based Approach to Smartphone Permission Requests” in February 2022. She has published a paper titled, An Investigation of Comic-based Permission Requests. In the 25th Nordic Conference on Secure IT Systems 2020.
Mike Just earned his Ph.D. in Computer Science from Carleton University in 1998 and is currently an Associate Professor at Heriot-Watt University. He is primarily interested in computer security, and in applying human-computer interaction and machine learning techniques to solve computer security problems. You can find more information at https://justmikejust.wordpress.com/
Tessa Berg graduated from the Heriot-Watt with a first class honours degree in Information Systems. She graduated in 2013 with a PhD in Rich Picture Interpretation. She lectured at Edinburgh Napier University before joining Heriot-Watt University. Currently working as School Director of Academic Quality and Associate Professor in Computing science. Additionally, she is actively involved in encouraging women into computer science.