End User Comprehension of Privacy Policy Representations

DOI:
10.1007/978-3-319-58735-6_10
10.1007/978-3-319-58735-6_10

Document Version
Accepted author manuscript

Published in:
End-user development : 6th International Symposium, IS-EUD 2017, Eindhoven, The Netherlands, June 13-15, 2017, Proceedings

End User Comprehension of Privacy Policy Representations

Sophia Kununka[1] (✉), Nikolay Mehandjiev [1], Pedro Sampaio [1] and Konstantina Vassilopoulou[2]

[1]Alliance Manchester Business School, The University of Manchester, Manchester, UK
sophia.Kununka@postgrad.mbs.ac.uk,
{n.mehandjiev,p.sampaio}@manchester.ac.uk
[2]Department of Informatics and Telematics, Harokopio University, Athens, Greece
kv@hva.gr

Abstract. The providers of mobile applications (apps) offer free apps and services but monetise user information and attention. However, end users (users) have limited control and inadequate understanding over the manner in which apps use their personal data. This study is a first step to taking a user centred approach in the design of app privacy policies to ensure they are easy to understand by non-technical users. To this end we capture the views of 41 users on four different privacy policy representations and analyse them to extract user priorities and needs. We have found that one of the alternative policy representations is liked best by users, and that users focused on data collection and use, neglecting other privacy aspects such as data monetisation and legal issues. As a result of our analysis, we propose a novel interactive representation to enhance the informativeness of privacy policies, especially with respect to data monetisation, whilst facilitating greater user control over personal data privacy. We evaluate our proposal using the cognitive dimensions framework.

Keywords. Mobile applications · Privacy policy · End user development

1 Introduction

Mobile apps process plentiful personal data that users provide with the confidence that data will be used for a limited set of purposes related to the functionality offered by the app. However, users have been observed consenting to uses such as marketing, exposure and renting of customer information, because these uses are obfuscated within long and difficult to understand privacy policies.

Customers favour privacy-friendly providers over privacy-invasive providers, however, customers are willing to purchase from privacy-invasive providers if they offer cheaper prices [1-2]. Irrespective of the level of privacy invasiveness of a customer-provider transaction, achieving an informed user choice requires users to clearly comprehend the intentions of service providers and the value they gain from allowing access to their data. This is empowering and streamlines user expectations with the extent to which they are willing to yield their privacy [3-4]. This is reinforced by regulatory bodies such as the US Federal Trade Commission and the

European Data Protection Act [5] that provide data protection guidance and, increasingly demand that app designers incorporate user privacy requirements into the design of apps. It is only natural that companies that neglect users' privacy concerns will inevitably face public anger over privacy [3]. In response, companies have begun to explore options such as provision of privacy policies and, adoption of business models that offer users trade-offs for their information.

Privacy policies aim to answer user privacy concerns, yet they are often designed from a service provider's perspective with a focus on validating compliance with regulators and fostering clients' confidence as opposed to facilitating user privacy transparency [6]. While privacy policies have been widely adopted, the traditional full length privacy policies face criticism for their complex and monolithic 'blanket' nature. The 'blanket' nature limits the options available to users to either accepting the entire policy or rejecting it, thus forfeiting the use of the app. App users feel a sense of hopelessness when faced with complex policies that offer them limited control over their privacy [7]. Further, users of mobile apps often want access to an app service in the shortest time possible and while users are concerned about their data privacy, they may not be willing to read the lengthy, time consuming and difficult to understand privacy policies. Likewise, mobile phone privacy usability concerns have also been cited [8], a complication that arises from constraints in the display interfaces which limit the amount of privacy information that can be displayed [6]. The necessity for simplification of privacy policies is clear.

We argue that to optimize user privacy representation in app policies, we need to find a balance where i) the privacy information representation is simplified, ii) users are provided sufficient information, iii) users are engaged with controlling privacy and iv) we can achieve a balance between monetisation interests of providers and privacy protection interests of users. To achieve this, a user centred design of privacy policies is required. The user centred design method seeks to incorporate meanful and relevant user input into system development [9].

In summary, this paper attempts to explore the representation of appropriate interactive mechanisms that allow users to be well informed so they can control their personal privacy. The rest of the paper is organized as follows: the section on related research is followed by a section describing the concept and the method of our study. We then present our results and conclude with discussion.

2 Related Research

2.1 Privacy Policy Representations

A number of proposals exploring solutions to the complexity of app privacy policies have been put forward with different degrees of success. Efforts in this area have included design of machine readable representations such as platform for privacy preferences [10] and privacy beacons [11]. Likewise, some approaches have involved studies to compare privacy policy representations that have at times yielded conflicting results. For instance, [12] reports that users favoured shorter and tabulated privacy policies over the full length policies (see Appendix) while [13] found that the full length policy was perceived as more secure and thorough by participants as compared

to other alternatives. The differences could be attributed to differences in context, while [12] focuses on enjoyability and ease of finding information in policy, [13] explored comprehension and perceptions on privacy security offered by policies.

However, both studies [12-13] confirm that full length policies yielded the worst accuracy results in terms of users' ability to find and correctly interpret privacy information, as compared to shorter alternative policy representations. This may be a pointer to inadequate user understanding of full length policies. A policy that lacks clarity, readability and is not clearly understood could lead to uninformed user privacy consent increasing opportunities for unanticipated and unwanted uses and disclosures of users' data. The preference of the full length policy in [13] could be attributed to users being hesistant to use policy representations that they are not familiar with and, as such bulding user trust for alternative policy representations may be attained through repeated use of new alternative policies and user education.

2.2 Privacy vs Monetisation Trade-Offs

Related research has studied how users' willingness to disclose their data is influenced by privacy policies [1]; mismatches between users' intention to share information and their actions [14] and trade-offs between privacy and personalization [15].

Achieving a balance in the mobile app ecosystem requires comprehension of the conflict of interests that exist between the service provider and the end user. The service provider is required to find equilibrium between privacy-preservation which greatly limits data monetisation and, privacy-invasiveness that monetises user data in order to ensure business viability [1]. In order to ensure clarity in a policy's privacy preservation or invasiveness, users should be facilitated with means of making and executing specific user choices regarding data monetisation. While privacy policies play a substantial role in expressing these conflicts, [16] stress that there is inadequate research on this subject. The willingness of users to share their data can be enhanced through incentives such as convenience or monetary benefits or discounts [17]. Hence while actual money may not be given to users, trade-offs between sharing their data and use of free apps could be facilitated. The requirement for further reseach into data handling approaches that optimize monetary and privacy interests such as pricing-by-privacy trade-offs have been recommended [1].

One of the shortcomings of the approaches that explore privacy policy representation development is that they fail to involve participants at the design level, engaging participants at the evaluation level. As such, participants' privacy perceptions are not captured into the design. A lack of user involvement in privacy policy design is an important gap in the development of user centred policies. Secondly, users are limited in understanding and control over the monetisation of their data. This study seeks to address these gaps and uniquely draws on end user development in policy design in the development of user centred app privacy policies that are simpler, and that innovatively facilitate more effective user controls and understanding while at the same time facilitating a means of enabling service providers to gain some monetary benefit.

3 Conceptual Framework

This study seeks to develop an end user centred privacy policy app design that simplifies the representation of privacy information and enhances user interaction and control over personal privacy. User centred design is compromised of four main stages: determination of user requirements, design, prototyping and assessment [9]. Our conceptual framework (shown in Fig. 1) incorporates the stages of the user centred design approach.

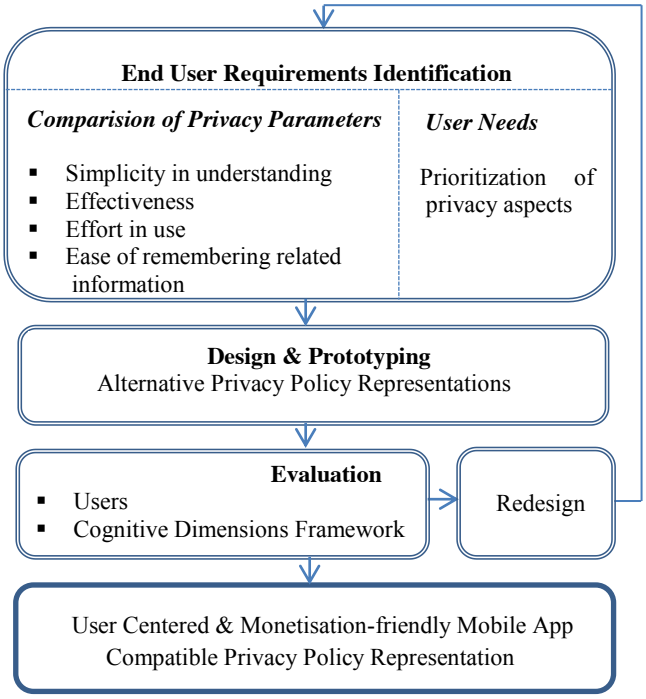


Fig. 1. Conceptual Framework of Study

The conceptualization of our conceptual frame began by exploring available literature on mobile privacy policies to identify areas of privacy concerns to users which we refer to as privacy parameters. The participants of the study were presented with several alternative privacy policy representations within a questionnaire survey and, were required to assess policy representatins against the privacy paramenters established from the literature. The participants' perceptions on the privacy parameters were used to guide the design and prototyping stages. Evaluation of the prototype design was conducted using the cognitive dimensions framework. This framework provides an outlook of the process perspective of a system and, is recommended as a

suitable means of assessing design artefacts in their intial phases [18]. The feedback received from the evaluation stage guided the prototype redesign through several iterations. The final output of the designg process was a user centred and monetisation-friendly privacy policy representation for mobile apps.

3.1 Privacy Representation Parameters Explored in the Study

Privacy policies have been criticised for their complexity [2], arising from the legal 'like' language used to relay information. This makes policies difficult for end users to understand. As such, we identified simplicity in understanding as one of the Privacy Representation Parameters to explore in this paper. Further, privacy policies are often deemed ineffective. Privacy should facilitate control over information sharing as opposed to not sharing [3]. This view is shared by [19] who assert that an effective privacy policy is one that enhances users' 'perceived control over their information disclosure and the secondary use of personal information'. Effectiveness is the second privacy parameter considered in our study.

Likewise, the length of policies is a deterant since reading policies is deemed by users to be a waste of time. A study [20] found that using an approximation of 244 hours a year, a normal user user would be required to invest two-thirds of an hour a day in reading privacy policies. Users often feel that reading policies is burdensome. This underpins the necessity of designing policies in a way that makes them effortless to read for the users.

In addition to the amount of user effort required, there is need to assess how easy users find it to find privacy relevant information in a policy. The granting of informed consent over user data requires that users are able to find information on the privacy areas they are particularly concerned about with ease. The current arrangement of privacy information in policies appears not to take this into consideration [21]. In total, four privacy representation parameters related to privacy policies were identified for the study namely: simplicity in understanding, effectiveness, effort in use, ease of remembering related information.

The privacy parameters were represented as Likert-scale questions to assess users' privacy perceptions on four alternative policy representations. The privacy policy representations were: the three best representations from the studies by [12-13] a policy representation that we developed. Based on the [12] study, we used the standardized table and the short text policy representation (see Appendix). The standardized table policy representation shows data collection versus data use and data sharing. It also uses different colours to signify default and non-default data collection and, clearly indicates optional data. The short text policy representation on the other hand is a textual natural language representation of the information presented by the standardized table representation, with related rows combined to ensure conciseness.

Further, we also used the goals and vulnerabilities policy representation in [13]. It is based on a traditional full length policy representation in which goals or vulnerability statements relevant to consumer privacy are bolded and highlighted. On mouse over, these statements present a pop up box with protection goals and vulnerabilities. The last representation was a design of our own, which we call the list format policy representation. It presents key privacy aspects together with a brief description of each aspect. In order to match current app business practices, the privacy aspects used

were established from a qualitative analysis of apps' privacy policy content from different business sectors such as: ecommerce, social networking, insurance, traffic and navigation etc. The key privacy areas in this representation included: required access, data security, user responsibilities, efforts in place to keep app free etc.

4 Method

4.1 Participants and Procedure

Participants were sourced online using Qualtrics [22] a statistical tool for data collection and analysis. Participants were offered £15 Amazon vouchers for their participation and were filtered based on gender, age, education and IT proficiency. A pilot study of 8 participants was conducted and the feeback received used to make improvements on the questionnaire.

Volunteers for the study were sought by email and provided a link to the Qualtrics. A total of 112 responses were received. The study plan covered 6 sessions inorder to control the numbers of participants. Particpants were selected based on their availabilty to commit to the available sessions, ruling out 59 of the potential participants. Another 14 responses were invalidated as 7 of them had invalid emails and could not be contacted while 5 contacted the study organize apologizing for a last minute cancealation. In total, 41valid responses were received for the study. Genderwise, we had hope participation close to 50% female and 50% male gender representation, while in terms of education we sought a representation of 10% A level, 30% Undergraduate and below, 30% masters and 30% PhD. We had also hope for a fairly equal distribution between the 3 age groups considered and a 50% IT proficiency and 50% other IT proficiency. The results obtained were differed from our initial expectatons but were useful nonetheless. The participants selected were aged 18 years and above to form a representative cross-section of skills, gender and education. Gender mix was 63.4% female and 36.6% male. Age statistics were 56.1% below 26 years, 43.9% between 26 – 36 years and, 2.4% above 36 years. Highest level of education statistics were 29.3% advanced level, 12.2% undergraduate, 48.8% masters, 7.3% PhD, 2.4% other. IT proficiency statistics were 0% none, 22% basic, 43.9% intermediate, 26.8% advanced, 7.3% expert.

A Spearman's correlation was conducted to explore any relationships between the participants' privacy preferences and the factors of age, gender and education. Only three statistically significant correlations were observed between gender and: the variant 2 – effectiveness factor (r_s =.333, $p < .05$), the variant 4 – effort factor (r_s =.400, $p < .05$) and, the variant 4 – remember factor (r_s =.321, $p < .05$) where r_s = coefficient. However, they were weak linear relationships and therefor no further tests conducted on them. As such, the weak relationships observed in the gender factor indicated that the gender imbalance in the sample population of this study has no significant effect on the participants' privacy preferences. Similarly, no significant relationships were observed between the demographic factors of age and education with the participants' preferences. As such further exploration of the preferences across their demographic population was deemed unnecessary.

The questionnaire was physically administered and conducted over two days separated by two weeks. Each day had three sessions, an hour and a half each. Three researchers were present throughout each session to explain any part of the questionnaire that was not clear to participants. Each session began with a brief presentation that introduced the purpose of the study, explained basic privacy concepts to participants and answered any questions by participants.

4.2 Design of the Questionnaire

We used the privacy policy of a fictitious app we called Jupiter X. The content of privacy information used in the Jupiter X app privacy policy was carefully selected so as to match it to real practices of companies. We presented its information as four different types of privacy policy representations. These were: the standardized table (R1), the short text (R2), the goals / vulnerabilities (R3) and, the list format (R4) respectively. Using a five point Likert scale, a questionnaire was then used to capture participants' perceptions on the different policy representations by assessing the policies in aspects of the four Privacy Representation Parameters: simplicity in understanding, effort required, effectiveness of policy, ease of remembering related information and lastly the participants' overall assessment of the policy representations. The Likert scales ranged from strongly disagree, disagree, neutral, agree, and strongly agree. While data collection could have been conducted using several approaches e.g. semi-structured interviews, this study used Likert scales were used because they are convinent and easily quantifiable. Due to Likert scales being subject to midline /outlier confusions and that participants may fake responses, participants were asked an open ended question as to why they had given the Likert scale responses. This encouraged them to think before providing Likert responses and also provided the researchers with more insight helpful in the interpretation of participants' responses. The findings contributed to development of improved user centred privacy policies.

In another task, participants were presented with a definition of a privacy policy and a brief description of six key areas privacy aspects found in privacy policies which were: data security, user rights, data collection, legal, data use, data exchanges (monetisation). They were then required to rank these privacy aspects according to which they considered the most important aspects on a scale of 1 (most important) to 6 (least important). This was conducted to capture what they considered to be the most important privacy aspects. Based on our findings we sought mechanisms of improving the areas of privacy elements in a policy that were ranked lowest. In particular, we assessed possible ways of enhancing the data exchanges (data monetisation) privacy aspect to make it more informative and interactive to users. Expert feedback was used to enhance our solution to ensure its effectiveness through several iterations. To this end, we developed an easily accessible interface linked to the data exchanges (data monetisation) that provides users with simplified understanding together with greater user control over the data monetisation aspect of privacy.

5 Results, Design Effort and Discussion

5.1 Variations of Policy Representations

Findings show that the most to the least 'simple to understand' policy representations were: R4, R2, R3 and R1 respectively. In terms of the least to the most required 'effort in use' were: R4, R2, R3 and R1 respectively, an outcome identical to the 'simple to understand' parameter. Results for the most to the least 'effective' policy representation were: R4, R2, R1 and R3. In light of 'ease of remembering related information', the easiest to remember to the most difficult were: R4, R1, R2 and R3 respectively. The overall assessment of the policy representations by the participants shows that ranking from the most agreeable to least agreeable representations were: R4, R2, R3 and R1 as shown in Table 4. R4 had the most user preference in terms of simplicity, effort, effectiveness and ease of remembering related information, followed by R2, R3 and R1 the least agreeable representation. A summary is shown in Table 1 with the abbreviations of the policy representations: the standardized table (R1), the short text (R2), the goals & vulnerabilities (R3), the list format (R4).

Table 1. User Preference of Policy Representations

	First	Second	Third	Fourth
Simplicity	R4	R2	R3	R1
Effortlessness	R4	R2	R3	R1
Effectiveness	R4	R2	R1	R3
Ease of Remebering	R4	R1	R2	R3
Overall Results	R4	R2	R3	R1

5.2 Ranking of Privacy Elements in Policy

Participants' ranking of the most to the least important privacy aspects in a policy were: data collection, data use, user rights, data security, data exchanges/monetisation and, legal respectively as shown in Fig. 2. The data exchanges/monetisation and the legal were considered the least important. Firstly, a possible explanation for the lowly ranked privacy aspects could be as a result of inadequate user understanding of these privacy aspects whereas participants may have ranked the most important privacy elements (data collection and use) as such because they felt they had a clearer understanding of these aspects. Both Android and iOS operating systems now offer greater permissions granularity during app installation through interfaces that highlight the user data collected together with the corresponding permissions to which users are required to consent for the download to continue. While there are several studies that indicate that there is inadequate user understanding of these permissions [24-25], permissions requirements give users a clearer idea of the data collected which contributes to user understanding and boosts user confidence. As such, user perceptions about the privacy aspects that were deemed as the least important could be improved by presenting these privacy aspects in more educative and easy to understand ways.

Secondly, the low importance ranking of legal and data exchanges/monetisation could also be an indicator that users feel that these aspects of privacy are out of their control and, thus indicating a need to introduce more user control in these areas. Research indicates that user trust, greater use and willingness to share data have been identified as one of the benefits of facilitating users with more control over their privacy [23]. Fig 2 shows users perceptions on the importance of privacy aspects: data security (DS), user rights (UR), data collection (DC), legal (L), data use (DU), data exchanges/monetisation (DE).

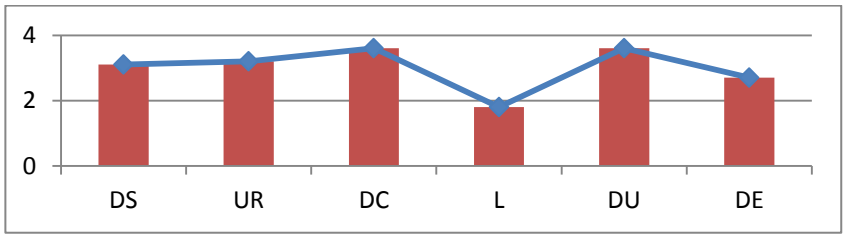


Fig. 2. Ranking of the Importance of Privacy Aspects in a Policy

5.3 Enhancements Contributed to Privacy Policy Representation

The list policy representation (R4) emerged as the most liked policy representation in our study. In order to achieve our goal of applying end user development in the design of app privacy policies, we integrated the insights gathered from our study on policy representations to further enhance the list policy (R4) producing our final proposed artefact. Fig. 3 and Fig. 4 depict a comparison between the initial List policy representation and the proposed artefact.

To evaluate our proposed artefact, we draw on the cognitive dimensions framework [18] that has been used to evaluate usability [24]. This framework according to [18] should not be confused for rules of design, but should be seen as a means of explaining the artefact-user relationship. Next, we present a discussion of the changes made to the list policy representation (R4) to generate our proposed artefact (see Fig. 3 and Fig. 4) in line with the relevant cognitive dimensions framework dimensions namely: Abstraction gradient, diffuseness, closeness of Mapping, visibility and juxaposability, secondary notation and escape from formalism, hidden dependencies, premature commitment, role expressiveness, viscosity, consistency, error-proness, hard mental operations and progressive evaluation.

The Jupiter X App **Details**	
Requires access to	Contacts information, demographic information, financial information, location information, cookie information
Why	To providing the service and maintenance of the site, profiling and support from other companies
To keep app free	We may monetize your data e.g. marketing
	Data may be revealed to others for research purposes
Data security measures	Data encryption, require staff to adhere the company's data privacy policy.
Your responsibility	Use strong, careful kept passwords
Your rights	Consent to data collection
	Access & update date, opt-out
Keeping your data	No more than 3 months after you opt-out
Changes in privacy policies	Email notification 7 days before change

Fig. 3. List Policy (as Used in Study)

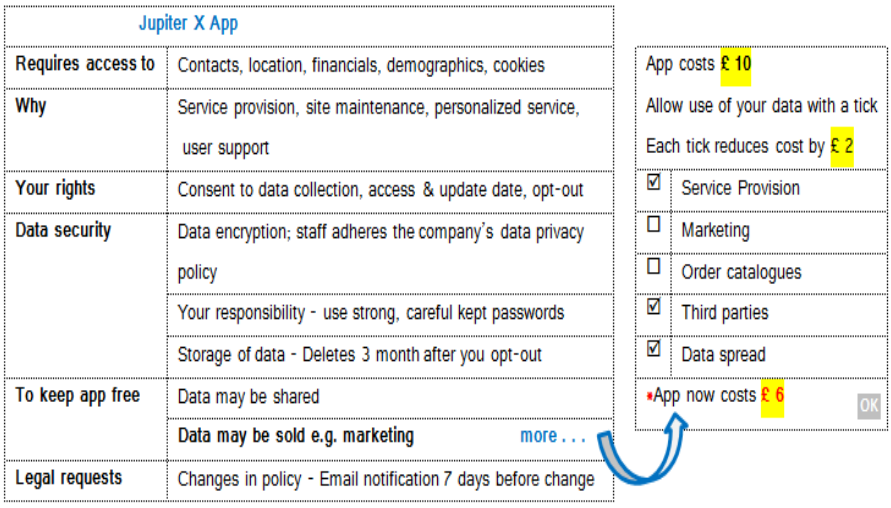


Fig. 4. Proposed artefact: New List Privacy Policy Representation

Abstraction Gradient. The abstraction dimension of the cognitive dimensions framework addresses the encapsulation or clustering of items into one to achieve simplicity. Depending on users' privacy concerns and it can be subdivided into three degrees of abstraction: abstraction hating, abstraction tolerant and abstraction hungry. Privacy freaks [14] are likely to follow under abstraction hating as they desire may much privacy information as possible, the average user is interested in privacy [6] given empowerment exercise it and is aligned with the abstraction tolerant and, the

abstraction hungry could represent careless users [8] users that take no thought of privacy either due to lack of awareness or interest. The relevance of representation is asserted by [3] who state that the transformation of data into information and thus the extent of its usability is greatly impacted by how the data is represented. A major focus in improving app privacy policy representations is content minimization due to the limitations of mobile phone interfaces. While a privacy balance is challenging to achieve we sought to attain a means of catering for the different abstractions that are represented by users.

Our artefact seeks to provide content minimization which is consistent with abstraction-hungry representation. To this end, the artefact presents privacy information in a tabular two column format that presents a particular privacy aspect with its brief description adjust to it. At the same time, our artefact seeks to cater for abstraction-tolerant by providing a more link to another interface with a brief description a particular privacy aspect such as the data monetisation. Further, for abstraction-hating, the full privacy policy is provided through an easily accessible link.

Diffuseness. Depending on the objective, representations may be tabular, graphical, textual, visual etc. The number of symbols or space required to convey information differs with different notations. In order to enhance readability the word count of sentences was reduced. The result is a reduction in the amount of information held in memory and as such facilitates faster information processing [8]. This facilitates better view of the policy on the limited mobile phone interfaces. Likewise, in some sections such the 'Why' section, comma separated key words were used to replace whole sentences therefore facilitating simpler relaying of privacy information.

Closeness of Mapping. The cognitive dimensions framework dimension of 'closeness of mapping' explores mapping of the problem world and a solution. Our artefact seeks to address the problem of representing privacy information such that it reflects what users deem as most important to their privacy problem. While there is limited research on the order in which privacy information is presented in a policy, [25] argue that the aspects of privacy that users are interested in differ. Based on our findings on their prioritisation of the different aspects of privacy information, our artefact rearranged the order in which privacy information is presented to users to reflect their needs. For instance, to highlight the key aspects of user privacy, the 'your rights' privacy aspect was moved from the bottom to third position in order of appearance. Our motivation here was to support informed consent as much as possible even in instances where users may be in a hurry to download apps. This enables them to quickly and easily access the aspects of privacy that are most important to them even in the event they do not want to explore all the privacy aspects of an app. In addition, the 'your responsibility' section was collapsed under the 'data security' privacy aspect where it rightfully belongs and also as a result makes the policy appearance less cluttered. The importance of this action is underpinned by [3] who state that 'every notation highlights some kinds of information at the expense of obscuring other kinds'.

Visibility and Juxaposability. The ability to display relevant information or provision of intuitive access to information or further being able to display related information adjust to each other is underlined in the visibility and juxaposbility dimension of the cognitive dimesnsion framework. This is particularly important due to the insummountable amount of information presented to users in traditional full length privacy policy representations. Specifically the 'To keep app free' section was developed to be more intuitive by appending a 'more' link at its right hand side (see Fig. 4). A study [26] recommends that simplified representations could have mechanisms through which users can obtain more comprehensive details should they be required. Juxaposability comes into effect by clicking the 'more' link, which provides an interface presenting a summary of several ways in which data may be monetized for instance: service provision, marketing, order catalogues, third parties, data spread etc. In addition, the interface displays the cost of the app which for example is £ 10. Further, it informs uses that they can consent to the different ways shown through which their data may be monetized by checking adjacent checkboxes. Users are also informed that for each type of data monetisation they consent to, the price of the app reduces by a certain amount for instance £ 2. At the bottom of that interface, the final cost of the app is automatically calculated and displayed based on the number of consent checks a user has provided. An 'ok' option together with an option to exit the interface is provided returning the user to the policy representation. Visibility and juxaposability are particularly important in helping address the challenge of how to improve users' perceptions of privacy aspects such as the data exchanges/monetisation which users ranked lowest in importance. By designing the artefact as described above, the data exchanges/monetisation was developed to be more informative and to facilitate greater user control over user privacy.

Secondary Notation and Escape from Formalism. The cognitive dimensions framework dimension of secondary notation and escapte from formalism focuses on how information may be relayed in unconventional ways. This could include use of aesthetics to enhance readability. The use of secondary notation has at times been critique as being a platform via which service providers try to influence users' by stressing certain information while ignoring what is 'truely' important to the users. However, our artefact seeks to support users in the in the privacy aspect of data exchanges/monetisation by using colour highlights to emphasis prices and checkboxes to indicate user consent and thus to facilitate user interactiveness and control over their privacy.

Hidden Dependencies. The cognitive dimensions framework dimension of 'hidden dependencies' which deals with exposing interdependencies between or within privacy aspects that may not be obvious to the users. Our enhancement of the data exchanges/monetisation privacy aspect is only a first step in dealing with this challenge. This is because while the user knows and thus consent on the ways in which their data may be monetised, they are not aware of how their data will spread out in the data market places espectially through third parties associated to the app/s they are using.

This is important as sensitive user data exposure without knowledgable consent could have significant consequences for instances health data [21]. This underpins the necessity for more research into how to express hidden dependencies in privacy policy representations.

Premature commitment. There are several instances or factors in privacy policy representation that could result in premature commitment or consent by users. As discussed earlier, hidden dependencies could be a contributing factor, the ordering of privacy information may be another contributer as a user may not be ready to ready the entire policy, or yet still the complexity and ambuiguity of privacy as it's represented in the traditional full length policy representation. The enhancements that our artefact proposes curb premature committement to an extent. However, research into user centred design of all the key privacy aspects in a policy is required in order to minimize premature commitment.

Other Dimensions in the Cognitive Dimensions Framework. The role expressiveness dimension addresses the ease of identitfying the use of each entity within the overall representation. In our artefact, role expressiveness is reflected through it structuring, use of secondary notation and and 'explicit description level' [18].

Viscosity another dimension deals with resistance to local and the amount of changes required to implement changes in a policy representation. Our artefact uses abstraction, a measure cited by [3] as a means of limiting user resistance.

Further, consistency is a dimension that deals with users' ability to infer a part of a representation from another earlier mastered representation part. Our artefact endeavours to maintain consistency by ensuring simplicity and a similar structuring throughout the representation.

Error-proness is a dimesion that enables recovery from mistakes. Whereas a user does not have the option of opting out once they agree to the traditional full length policy, our enhanced data exchanges/monetisation facility enables users not only to careless express their choices or also to cancel or change any undesired option.

The hard mental operations dimension addresses the degree of mental processing necessary as opposed to the semantic process. Our artefact seeks to limit the effort of mental processing involved in the use of the representation as this eases understanding. Hence the artefact design involved the simplifion of terminologies that participants had identified as 'jargons'. For example, the statement 'we may monetize your data' was changed to 'we may sell some of your data', 'profiling' changed to 'personalized service' etc. The last dimension, progressive evaluation was conducted by seeking expert feedback during the design process. The artefact went through several processes of refininement enhancing its effectiveness in privacy policy representation.

6 Conclusion and Future Work

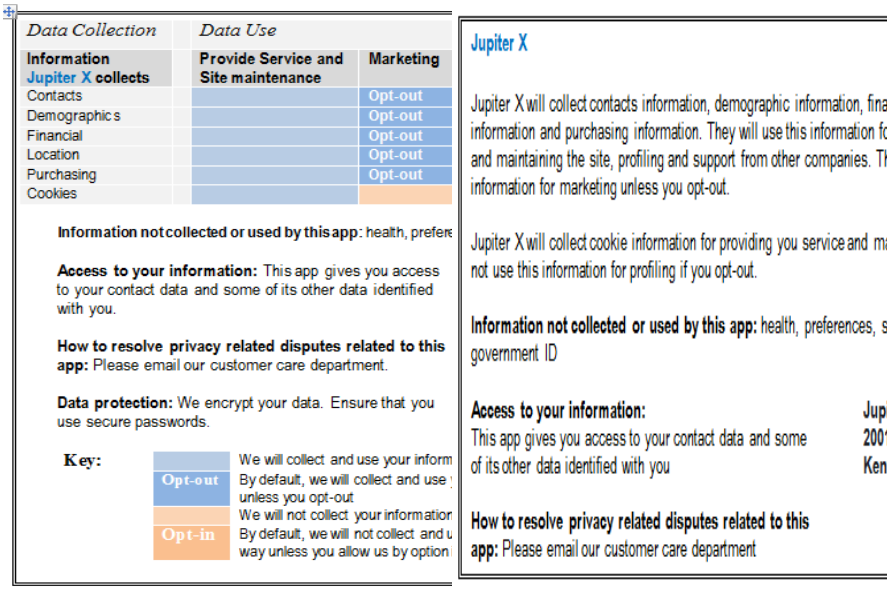
We use a user-centred approach in designing a privacy policy representation which balances information with ease-of-understanding, and allows communicating important monetisation trade-offs to end users. Drawing on literature, we establish privacy representation parameters that are pertinent for achieving a more usable and thus effective privacy policy design. A study of 41 users assessed four privacy policy representations using the privacy representation parameters. The most preferred privacy policy representation by users was the list policy representation, followed by the short text policy representation, then the goals and vulnerabilities policy representation and last was the standardized table policy representation.

Users' focus was mainly on the data collection and use as opposed to the data monetisation and legal privacy aspects. We propose a solution to enhance the limited understanding of the data monetisation aspect and checked its usability using the cognitive dimensions framework. The end result is a privacy policy representation that empowers user to provide more informed consent about the use of their personal information and facilitaties user interaction and control over the data monetisation privacy aspects. In future research we plan to investigate ways of refining and testing the language or terminology used so as to further enhance user understanding.

Appendix

R 2: The short text policy

R 1: The standardized table policy



Data Collection	*Data Use*	
Information Jupiter X collects	**Provide Service and Site maintenance**	**Marketing**
Contacts		Opt-out
Demographics		Opt-out
Financial		Opt-out
Location		Opt-out
Purchasing		Opt-out
Cookies		

Information not collected or used by this app: health, prefere

Access to your information: This app gives you access to your contact data and some of its other data identified with you.

How to resolve privacy related disputes related to this app: Please email our customer care department.

Data protection: We encrypt your data. Ensure that you use secure passwords.

Key:

	We will collect and use your inform
Opt-out	By default, we will collect and use unless you opt-out
	We will not collect your information
Opt-in	By default, we will not collect and u way unless you allow us by option

Jupiter X

Jupiter X will collect contacts information, demographic information, fina information and purchasing information. They will use this information fo and maintaining the site, profiling and support from other companies. Th information for marketing unless you opt-out.

Jupiter X will collect cookie information for providing you service and ma not use this information for profiling if you opt-out.

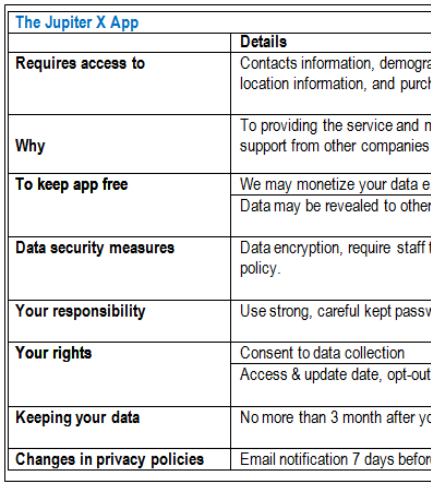
Information not collected or used by this app: health, preferences, s government ID

Access to your information:
This app gives you access to your contact data and some of its other data identified with you

Jup
200
Ken

How to resolve privacy related disputes related to this app: Please email our customer care department

R 3: The goals / vulnerabilities policy **R 4** : The list policy



The Jupiter X App	
	Details
Requires access to	Contacts information, demogra location information, and purch
Why	To providing the service and n support from other companies
To keep app free	We may monetize your data e Data may be revealed to other
Data security measures	Data encryption, require staff t policy.
Your responsibility	Use strong, careful kept passv
Your rights	Consent to data collection Access & update date, opt-out
Keeping your data	No more than 3 month after yo
Changes in privacy policies	Email notification 7 days befor

References

1. Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. Gerlach, J, Widjaja, T and Buxmann, P. 1, 2015, The Journal of Strategic Information Systems., Vol. 24, pp. 33-43.
2. Study on monetising privacy: An economic model for pricing personal information. Jentzsch, N, Preibusch, S and Harasser, A. 2012. ENISA.
3. The economics of privacy. Acquisti, A, Taylor, C.R and Wagman, L. 2016.
4. Taylor, Chris and Webb, Ron. A Penny for Your Privacy? HBR BLOG NETWORK. [Online] 2012. [Cited: 6 1 2017.] http://blogs.hbr.org/cs/2012/10/a_penny_for_your_privacy.html.
5. Data privacy approaches from US and EU perspectives. Steinke, G. 2, 2002, Telematics and Informatics, Vol. 19, pp. 193-200.
6. A design space for effective privacy notices. Schaub, F, et al., et al. 2015. Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 1-17.
7. Reflection or action?: How feedback and control. Patil, S, et al., et al. s.l. : 2014, 2014. CHI .
8. Can Adaptive Interfaces Improve the Usability of Mobile Applications? Wesson, J.L, Akash, Singh and Tonder, Bradley van. Brisbane : Human-Computer Interaction , 2010.
9. Sharp, H, Rogers, Y and Preece, J. Interaction design: beyond human-computer interaction. 2nd. West Sussex : John Wiley & Sons, 2006.
10. P3P. Platform for privacy preferences. [Online] 2007. [Cited: 6 1 2017.] https://www.w3.org/P3P/.

11. Privacy by design - Principles of privacy-aware ubiquitous systems. Langheinrich, M. s.l. : Springer Berlin Heidelberg, 2001. Ubicomp 2001: Ubiquitous Computing. Vol. 2201 , pp. 273 - 291.
12. Standardizing privacy notices: an online study of the nutrition label approach. Cranor, Lorrie, et al., et al. s.l. : ACM, 2010. Human Factors in Computing Systems: Proceedings of the SIGCHI Conference. pp. 1573-1582.
13. Privacy policy representation in web-based healthcare. Earp, J.B, Vail, M and Anton, A.I. [ed.] System Sciences. s.l. : IEEE, 2007. 40th Annual Hawaii International Conference. pp. 138-138.
14. Privacy Attitudes and Privacy- Related Behavior. Norberg, P.A and Horne, D.R. 10, 2007, Psychology & Marketing, Vol. 24, pp. 829-847.
15. Willing to pay for quality personalization? Trade-off between quality and privacy. Li, T and Unger, T. 6, 2012, European Journal of Information Systems, Vol. 21, pp. 621-642.
16. Privacy in the digital age: a review of information privacy research in information systems. Bélanger, F and Crossler, R.E. 4, 2011, MIS quarterly, Vol. 35, pp. 1017-1042.
17. Why would we care about privacy? Dinev, T. 2, 2014, EJIS, Vol. 23, pp. 97-102.
18. Usability Analysis of Visual Programming Environments: A 'Cognitive Dimensions' Framework. Green, G and Petre, M. 2, 1996, Journal of Visual Languages and Computing, Vol. 7, pp. 131-174.
19. Trust factors influencing virtual community members: A study of transaction communities. Wu, J.J, Chen, Y.H and Chung, Y.S. 9, 2010, Journal of Business Research, Vol. 63, pp. 1025-32.
20. The cost of reading privacy policies. McDonald, A.M and Cranor, L.F. s.l. : ISJLP, 2008. Vol. 4, p. 543.
21. Expectation and purpose:understanding users' mental models of mobile app privacy through crowdsourcing. Lin, J, et al., et al. s.l. : ACM UbiComp, 2012.
22. Qualtrics. Welcome to the qualtrics experience management platform. Qualtrics.com. [Online] Qualtrics, 2017. [Cited: 15 3 2017.] https://www.qualtrics.com/.
23. Misplaced confidences privacy and the control paradox. Brandimarte, L, Acquisti, A and Loewenstein, G. 3, 2013, Social Psychological and Personality Science, Vol. 4, pp. 340–347.
24. Using the cognitive dimensions framework to evaluate the usability of a class library. Clarke, S and Becker, C. s.l. : First Joint Conference of EASE PPIG (PPIG 15), 2003.
25. Nielsen, Jakob. 10 Usability Heuristics for User Interface Design. www.nngroup.com. [Online] 1 1 1995. [Cited: 8 3 2016.] https://www.nngroup.com/articles/ten-usability-heuristics/.
26. End User Service Composition: Perceptions and Requirements. Mehandjiev, Nikolay, et al., et al. 2010. 2010 Eighth IEEE European Conference on Web Services. pp. 139-146.