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@hua.gr

Abstract. Providers of mobile applications (apps) offer free apps and services but monetise user information and attention, whilst app 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 tend to believe will only be used for a limited set of purposes related to the functionality offered by the app. However, privacy policies tend to state much wider purposes such as marketing, exposure and renting of customer information, and users have been observed to consent to these purposes, which are obfuscated within long and difficult to understand and policies.

Customers are known to favour privacy-friendly providers over privacy-invasive providers, yet the same customers are willing to purchase from privacy-invasive providers if they offer cheaper prices [1, 2]. Achieving an informed user choice thus necessitates that users comprehend the intentions of service providers with respect to personal data, and the value gained by users in exchange for allowing access to their data. This would align user expectations with the extent to which they are willing to

S. Barbosa et al. (Eds.): IS-EUD 2017, LNCS 10303, pp. 135–149, 2017.
DOI: 10.1007/978-3-319-58735-6_10

yield their privacy [3, 4]. Clarity regarding the use of personal data is reinforced by regulatory bodies such as the US Federal Trade Commission and the European Data Protection Act [5], which provide data protection guidance and, increasingly demand that app providers incorporate user privacy requirements into the design of apps. Indeed companies that neglect users' privacy concerns face public anger [3] and the provision of explicit privacy policies is now common, together with the adoption of business models that offer users trade-offs for their information.

Privacy policies are meant 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 content and 'blanket' nature. The 'blanket' nature limits the options available to users to either accepting the entire policy or rejecting it, the latter choice 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 the way privacy is represented in app policies, we need to find a balance point in the design space where (i) the privacy information representation is simplified, (ii) users are provided with sufficient information about how their data is used and why, (iii) users can consent to specific elements of the policy, and (iv) users understand the trade-off between monetisation interests of providers and privacy protection interests of users. To achieve this, a user centred approach to the design of privacy policies is needed, indeed we are using a user centred design method to incorporate meaningful 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. The paper then presents our results and concludes 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 a platform for privacy preferences [10] and privacy beacons [11]. User studies comparing privacy policy representations do exist although some have 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.

These differences are logical when considering the focus of the two studies, indeed [12] focuses on enjoy ability 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 yield 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 building 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 research 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 existing approaches to developing privacy policy representations is that they engage participants at the evaluation stage rather that at the design stage. 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 how their data is monetized and they cannot control this. This study seeks to address these gaps and uniquely draws on the academic area of end user development, seeking to involve non-technical users in the design of effective privacy representations. The aim is to create a user-centred privacy representation that is simpler, easier to comprehend,

facilitates effective user control of their personal data whilst allowing service providers to use business models based on monetizing personal information.

3 Conceptual Framework

This study seeks to design a user-friendly privacy policy representation that facilitates user comprehension and control over personal privacy. We follow the user centred design process [9] with its four main stages: determination of user requirements, design, prototyping and assessment. However, the results reported here are from the first iteration through the process, where the focus is on user requirements and preferences, and the other stages are simplified, involving the design and heuristic evaluation of a simple static prototype of the representation. The results will be fed into a second iteration through the process which will focus on producing a high-fidelity interactive prototype and evaluating it through user observation studies.

Our conceptual framework (shown in Fig. 1) incorporates the stages of the user centred design process, focusing on the first iteration through the process.

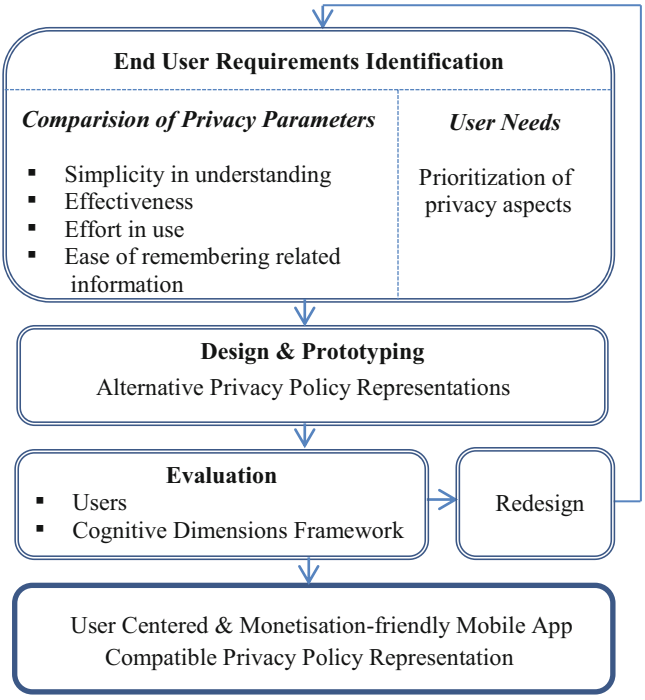


Fig. 1. Conceptual framework of study

Our work 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 four alternative privacy policy representations within a questionnaire survey. Three of policy representations were sourced from the literature while the fourth was a design of our own based on qualitative analysis of app privacy policies. Participants were asked to assess the policy representations against the privacy parameters established from the literature. The participants' most liked policy representation from our study was identified. This representation was then used in the design and prototyping stages as a basis to develop the prototype of the final design version presented in this paper which was guided by the participants' opinions regarding the privacy parameters and their representation choices. Evaluation of the prototype design was conducted using the cognitive dimensions framework [18], which is recommended as a suitable means of assessing design artefacts in their initial phases. The feedback received from the evaluation stage is presented here and will be used to guide the next iteration of the prototype design, aiming towards 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], partially arising from the language used to relay information which uses legal terms and structure. This makes policies tuned to demonstrating statutory compliance and hence difficult for non-specialists to understand. As such, we identified *simplicity in understanding* as the first privacy representation parameter to explore in this study.

Further, privacy policies are often deemed ineffective, since they fail to facilitate control by users over information 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 therefore 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 and burdensome. A study [20] found that a typical user would be required to invest 40 min per day for reading privacy policies. This underpins the necessity of designing policies in a way that reduces the effort to read them required from the users. *Effort in use* is thus the third parameter in our study.

In addition to the amount of user effort required, there is a need to assess how easy it is for users to find specific privacy-related information in a policy. This is to facilitate the granting of informed consent over the user of personal data. However, the current arrangement of privacy information in policies appears not to take this into consideration [21]. *Ease of remembering related information* in the policy is thus the fourth parameter in our study.

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 Cranor et al. [12] and Earp et al. [13] plus an initial version of an alternative policy representation that we developed.

The first two representations were based on the Cranor et al. [12] study: the *standardized table policy representation* and the *short text policy representation* (see Appendix). The standardized table 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* from Earp et al. [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 an initial design of our own, called the *list format policy representation*. It presents key privacy aspects together with a brief description of each aspect. The set of privacy aspects used were established as a result of our qualitative analysis of 100 privacy policies from different business sectors such as: ecommerce, social networking, insurance, traffic and navigation etc.

4 Method

4.1 Participants and Procedure

Participants were sourced online using an email with a hyperlink to a filtering questionnaire developed in Qualtrics [22]. Participants were offered £15 Amazon vouchers for their participation. A pilot study of 8 participants was conducted and the feedback received used to make improvements on the questionnaire.

A total of 112 responses were received. These were filtered according to availability for scheduled sessions, validity of contact details, gender, age, education and IT proficiency, leaving 41 valid responses with mixed demographics. Gender mix was 63% female and 37% male. Age was under 26 years for 56%, 44% between 26–36 years and 2% above 36 years. In terms of highest level of education attainted, 29% had advanced level, 12% undergraduate, 49% masters, 7% PhD, 2% other. IT proficiency statistics were 22% basic, 44% intermediate, 27% advanced, 7% expert.

Spearman's correlation was used to determine if demographics in terms of age, gender and education impact privacy preferences. Only three statistically significant correlations were observed between gender and privacy preferences: 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 therefore no further tests were 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.

Each selected participant completed the questionnaire within one of the the six scheduled sessions. Three researchers were present throughout each session to explain any part of the questionnaire that was not clear to participants. Each session began with an identical 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 an example of 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 the 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 mixture of open-ended questions and five point Likert scale questions, the questionnaire captured participants' perceptions on the different policy representations in respect 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 open ended questions invited participants to qualify the responses they provided on the Likert scale questions. This encouraged them to reflect on and consider their answers 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 privacy aspects found in privacy policies: data security, user rights, data collection, legal, data use, data exchanges (monetisation). They were then required to rank these privacy aspects according to their importance.

4.3 Design and Evaluation of a Prototype Representation

Based on our findings we designed a prototype representation which was based on the most-liked representation and addressed the user needs identified. For example we sought mechanisms of improving the areas of privacy elements in a policy that were least understood and cared for by users. The solution was then evaluated using the cognitive dimensions framework of heuristic evaluation [18].

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

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 Identifying	R4	R1	R2	R3
Overall Results	R4	R2	R3	R1

were: R4, R2, R1 and R3. In light of 'ease of identifying related information', the easiest 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 preferred to least preferred representations were: R4, R2, R3 and R1 as shown in Table 1. 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).

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 [17, 23], 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 educational 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].

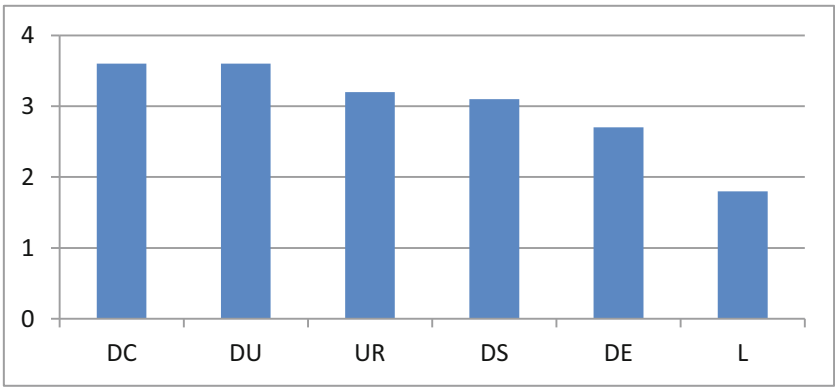


Fig. 2. Ranking of the importance of privacy aspects in a policy

5.3 Enhancements Contributed to Privacy Policy Representation

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. The cognitive dimension framework has the following dimensions: 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. Next, we present a discussion on the evaluation of our design based on these dimensions.

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 fall under the "abstraction hating" category 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" category and, the "abstraction hungry" category could represent careless users [8], which 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

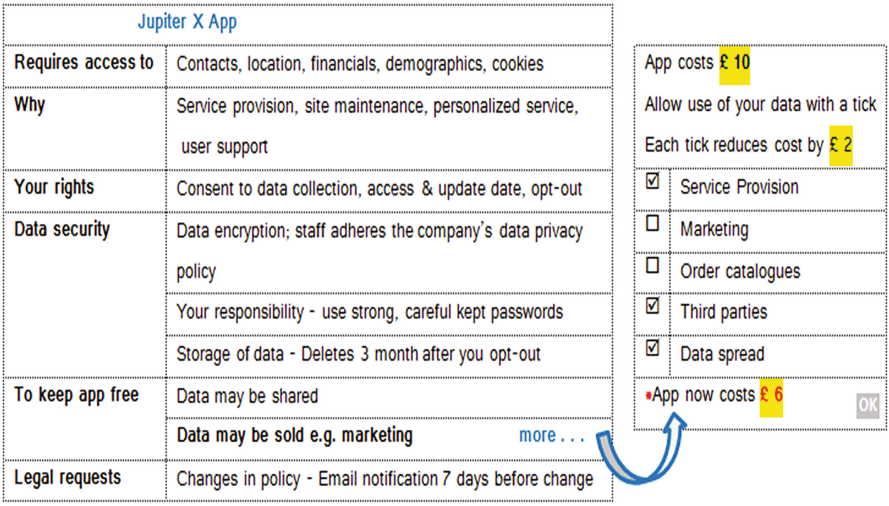


Fig. 3. Proposed artefact: new list privacy policy representation

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 (Fig. 3).

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 dimension framework. This is particularly important due to the insurmountable 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. 3). 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 escape 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 especially 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 contributor as a user may not be ready to ready the entire policy, or yet still the complexity and ambiguity 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 identifying 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 dimension 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.

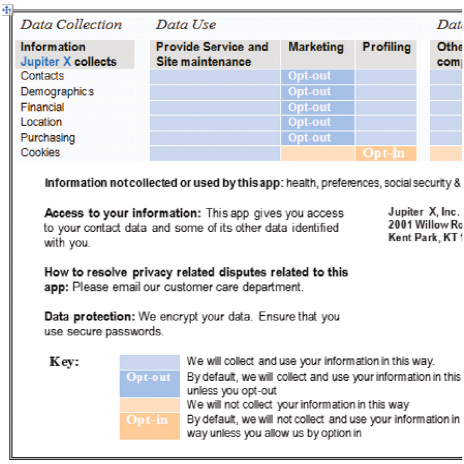
6 Conclusion and Future Work

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 facilitates 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 1: The standardized table policy



Data Collection *Data Use* *Dat*

Information Jupiter X collects	Provide Service and Site maintenance	Marketing	Profiling	Othe com
Contacts		Opt-out		
Demographics		Opt-out		
Financial		Opt-out		
Location		Opt-out		
Purchasing		Opt-out		
Cookies			Opt-in	

Information not collected or used by this app: health, preferences, social security &

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

Jupiter X, Inc.
2001 Willow Rc
Kent Park, KT

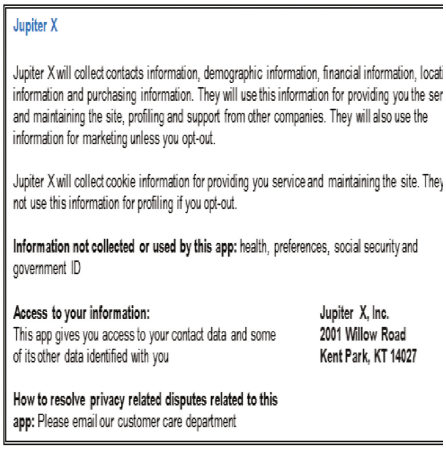
How to resolve privacy related disputes related to this app: Please email our customer care department.

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

Key:

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

R 2: The short text policy



Jupiter X

Jupiter X will collect contacts information, demographic information, financial information, locati information and purchasing information. They will use this information for providing you the ser and maintaining the site, profiling and support from other companies. They will also use the information for marketing unless you opt-out.

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

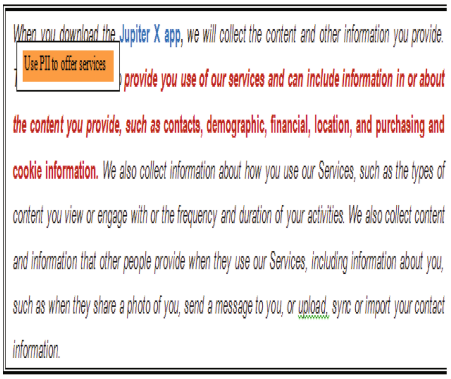
Information not collected or used by this app: health, preferences, social security and government ID

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

Jupiter X, Inc.
2001 Willow Road
Kent Park, KT 14027

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

R 3: The goals and vulnerabilities policy



R 4 : The list format policy

The Jupiter X App	
	Details
Requires access to	Contacts information, demographic information, fina location information, and purchasing and cookie inf
Why	To providing the service and maintenance of the sit support from other companies
To keep app free	We may monetize your data e.g. marketing Data may be revealed to others for research purpos
Data security measures	Data encryption, require staff to adhere the compan 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 month after you opt-out
Changes in privacy policies	Email notification 7 days before change

References

1. Gerlach, J., Widjaja, T., Buxmann, P.: Handle with care: how online social network providers' privacy policies impact users' information sharing behavior. J. Strateg. Inf. Syst. **24**(1), 33–43 (2015). doi:10.1016/j.jsis.2014.09.001
2. Jentzsch, N., Preibusch, S., Harasser, A.: Study on monetising privacy: an economic model for pricing personal information. In: ENISA (2012)
3. Acquisti, A., Taylor, C.R., Wagman, L.: The economics of privacy (2016). doi:10.1257/jel.54.2.442
4. Taylor, C., Webb, R.: HBR Blog Network (2012). http://blogs.hbr.org/cs/2012/10/a_penny_for_your_privacy.html
5. Steinke, G.: Data privacy approaches from US and EU perspectives. Telematics Inform. **19** (2), 193–200 (2002)
6. Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F.: A design space for effective privacy notices. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), pp. 1–17 (2015)
7. Patil, S., Schlegel, R., Kapadia, A., Lee, A.J.: Reflection or action? How feedback and control. In: CHI (2014). doi:10.1145/2556288.2557121
8. Wesson, J.L., Akash, S., van Tonder, B.: Can Adaptive Interfaces Improve the Usability of Mobile Applications? Brisbane (2010). doi:10.1007/978-3-642-15231-3_19
9. Sharp, H., Rogers, Y., Preece, J.: Interaction Design: Beyond Human-Computer Interaction, 2nd edn. Wiley, West Sussex (2006)
10. P3P. Platform for privacy preferences (2007). https://www.w3.org/P3P/
11. Langheinrich, M.: Privacy by design — principles of privacy-aware ubiquitous systems. In: Abowd, Gregory D., Brumitt, B., Shafer, S. (eds.) UbiComp 2001. LNCS, vol. 2201, pp. 273–291. Springer, Heidelberg (2001). doi:10.1007/3-540-45427-6_23
12. Cranor, L., Kelley, P.G., Cesca, L., Bresee, J.: Standardizing privacy notices: an online study of the nutrition label approach. In: Human Factors in Computing Systems: Proceedings of the SIGCHI Conference, pp. 1573–1582 (2010). doi:10.1145/1753326.1753561

13. Earp, J.B., Vail, M., Anton, A.I.: Privacy policy representation in web-based healthcare. In: 40th Annual Hawaii International Conference, p. 138 (2007). doi:10.1109/HICSS.2007.445
14. Norberg, P.A., Horne, D.R.: Privacy attitudes and privacy-related behavior. Psychol. Market. **24**(10), 829–847 (2007)
15. Li, T., Unger, T.: Willing to pay for quality personalization? Trade-off between quality and privacy. Eur. J. Inf. Syst. **21**(6), 621–642 (2012). doi:10.1057/ejis.2012.13
16. Bélanger, F., Crossler, R.E.: Privacy in the digital age: a review of information privacy research in information systems. MIS Q. **35**(4), 1017–1042 (2011)
17. Dinev, T.: Why would we care about privacy? EJIS **23**(2), 97–102 (2014). doi:10.1057/ejis.2014.1
18. Green, G., Petre, M.: Usability analysis of visual programming environments: a 'cognitive dimensions' framework. J. Visual Lang. Comput. **7**(2), 131–174 (1996). doi:10.1006/jvlc.1996.0009
19. Wu, J.J., Chen, Y.H., Chung, Y.S.: Trust factors influencing virtual community members: a study of transaction communities. J. Bus. Res. **63**(9), 1025–1032 (2010). doi:10.1016/j.jbusres.2009.03.022
20. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. J. Law Policy Inf. Soc. (ISJLP) **4**, 543 (2008)
21. Lin, J., et al.: Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing (2012). doi:10.1145/2370216.2370290
22. Qualtrics. Qualtrics.com (2017). https://www.qualtrics.com/
23. Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced confidences privacy and the control paradox. Soc. Psychol. Pers. Sci. **4**(3), 340–347 (2013)
24. Clarke, S., Becker, C.: Using the cognitive dimensions framework to evaluate the usability of a class library (2003)
25. Nielsen, J.: (1995). www.nngroup.com, https://www.nngroup.com/articles/ten-usability-heuristics/
26. Mehandjiev, N., Namoune, A., Wajid, U., Macaulay, L., Sutcliffe, A.: End user service composition: perceptions and requirements. In: Eighth IEEE European Conference on Web Services, pp. 139–146 (2010)