Probing the Design Space of Usable Privacy Policies: A Qualitative Exploration of a Reimagined Privacy Policy

Rhianne Jones
BBC Research and Development
MediaCity, UK
Rhia.jones@bbc.co.uk

Neelima Sailaja
University of Nottingham
Nottingham, UK
Neelima.sailaja@nottingham.ac.uk

Lianne Kerlin
BBC Research and Development
MediaCity, UK
Lianne.Kerlin@bbc.co.uk

This paper explores the design space of privacy policies through the prototyping of a 'reimagined' privacy policy for a UK media service. Privacy policies notify potential users about the data practices of a service and, in principle, enable users to make informed decisions about how their data is used. In practice, they are routinely ineffective, by design. In response to the persistent problems with the effectiveness of privacy policies we develop a prototype of a 'reimagined' privacy policy for a UK media service. We conduct several workshops with stakeholders to explore the problems with existing policies and identify how they could better balance industry and user needs and use these findings to prototype a new interactive policy design for the service. Our prototype presents a new visual design and added options and controls for data exchange. We conduct an exploratory study with potential service users to explore how the prototype compares with an existing policy, eliciting feedback on the visual design and control options before facilitating a discussion about users' past experiences and needs in relation to the policy design space. Findings from the pilot study show participants appreciated key elements of the new design and valued the new options for sharing data with service providers and restricting data collection and use - negotiating 'degrees of consent'. Findings suggest people felt more empowered by the design and this improved their impression of the service provider in terms of openness, fairness and trustworthiness. The paper contributes to HCI by advancing our understanding of the potential of the design space to increase engagement with privacy policies and in the data exchange process. This paper does not promote this design per se as a solution but uses it as a vehicle to discuss the potential of reimagining the design space for policies.

Usable Privacy; Visual Design; Data Negotiations; Interviews; Human Data Interaction

1. INTRODUCTION

Privacy is considered an essential value around the world and recognised as a human right (Solve 2009). Privacy principles and laws are rooted in the notion of individual control. Westin's (1967:7) notion of privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others', is often cited as a historical marker of this. Providing notice is an essential aspect of privacy and data protection legislation requiring legal and regulatory compliance. European Data Protection directives (EU directive 1995; 2002) have made it mandatory to provide users with privacy policies to ensure ethical exchange of data. A privacy notice is a public announcement to notify a user about the data practices of a service. They disclose information about the collection, processing, retention, and sharing of data linked to a user profile (ICO 2017). In principle, this is to help the user make an informed decision regarding the use of their data but in practice they are ineffective - by design (Calo: 2012; Jenson and Potts 2004; Schaub et al; 2015; McDonald and Cranor 2008).

Privacy notice and choice continue to be key principles of privacy protection (ICO 2017). However, policies serve multifaceted and contradictory roles to different parties (see Schuab et al. 2015). Their obligations to potential users are one of several functions they serve. They provide legal protection to companies as well as essential records for regulators to hold companies to account (ibid: 2). This 'conflation of requirements' (Schaub et al. 2015:2) has resulted in a catalogue of complaints against privacy policies from a user perspective, e.g. for being long-winded, written in legal jargon and not giving users adequate control. They are criticised for providing legal protection to companies and for routinely failing to meet their obligations to end-users (See Cranor 2012; McDonald and Cranor 2008; Schaub et al. 2015; Calo 2012).

Regulators and privacy advocates forcefully argue for urgent improvements and on-going efforts to tackle these problems. Current guidance aims to make policies more understandable so people can exercise better judgement and make decisions. Advice is also given on how to give users adequate choice and control in the process, to determine how their data is used (ICO 2017b). This guidance includes, the use of clear language, getting rid of jargon, only including essential information, and offering users meaningful controls (ICO 2017b).

The European Commission (EC) and the US Federal Trade Commission (FTC) have identified privacy by design (Cavoukian 2009) as playing a crucial role in approaches to data protection and privacy (See Ramirez 2012). In 2012, the FTC included privacy by design in their privacy framework as one of three key recommendations to businesses and policy makers for the protection of personal data (see FTC 2012). This approach to privacy aims to connect privacy regulation to design practice with the core goal of designing privacy into the system (Cavoukian 2009). At the same time, large companies (e.g. Google and Facebook) have begun to integrate policy information and privacy settings. New privacy 'hubs' or 'centres' could represent a move towards more user-centred, interactive privacy policies and provisions, away from the traditional static text-based policies.

Given the above, there is a clear need for ongoing user-centred research into privacy policy design. We take an existing policy for a UK media service and create a 'reimagined' version, which presents a new visual design and controls for helping users to negotiate data exchange with service providers. We focus on a UK media service, in response to persistent problems with the effectiveness of current industry privacy policies. Our reimagined design significantly diverged from the largely text-based policy that was in place prior to the study.

We use the term '*reimagined policy*' to capture the process of taking an existing privacy policy used by a company and creating an alternative version, that represents how that policy could be otherwise – with a view to better balancing the needs of users and service providers. Simply speaking, to help explore how policies can better serve users. This process consisted of identifying problems and potential solutions and design work experimenting with new visual design techniques and controls, and alternative models for users to share/restrict data in exchange for use of a service - rooted in ideas about more negotiable models for data exchange. We argue that re-envisioning an existing service privacy policy can push boundaries of creative thinking in industry beyond the status quo, to advance current understandings of the design space in specific service contexts.

We conduct several workshops with stakeholders to explore the problems with existing policies and potential solutions and begin design work on how policies could be created differently to better improve how policies adhere to, and balance, their obligations to users and service providers. We use the findings from these workshops to prototype a new interactive privacy policy for the service.

To evaluate whether our prototype was successful in its aims, we conduct an exploratory study with service users to explore the new design and discuss how it compares with a previous privacy policy the company had been using. We invited people to come and preview two new interactive content pilots for the service. Participants were shown both the reimagined policy and the existing policy in the service context. We recorded how people interacted with the two policies and conducted semi-structured interviews and walkthroughs to elicit feedback and reflections on the new policy design and foster an open discussion about privacy policies, for example, in terms of barriers to use and opportunities to better serve users.

Participants reported key benefits to the new design including higher levels of interest and engagement with the policy, self-reported improvements in their awareness of company data practices and a greater satisfaction with the level of control they were afforded. The findings suggest users felt more empowered by the design and that this improved their perception of the openness, fairness and trustworthiness of the service. The paper contributes to HCI by advancing our understanding of the potential of the design space to increase engagement with privacy policies and to re-think the data exchange process. We do not promote this design per se as a solution but use this research as a vehicle to discuss the potential for reimaging privacy policies.

This work was undertaken in a large-scale UK media organisation in a research and development department in 2016. It is intended to support the organisation in future phases of policy redesign. It aligns with its commitment to improving engagement with policies. This study was conceived of and conducted to generate a timely example of the value that can be derived from research and innovation in this area, helping to justify industry time and effort expended in developing practical solutions to the longstanding problem of ineffective policy design and user disengagement with policies.

2. BACKGROUND & RELATED WORK

2.1 Privacy Behaviours

People's privacy preferences are complex and nuanced and vary according to the type of data, the service (Bilogrevic and Ortlieb 2016) and the context in which data is disclosed (Nissenabaum 2010: 129-157; Marwick and Boyd 2014). Other factors that shape privacy preferences include degrees of trust in a company (Bilogrevic and Ortlieb 2016) and levels of interest in reading policies (McDonald and Cranor 2008). We also see persistent irregularities between privacy attitudes and behaviours, (Barnes 2006) whereby high levels of interest and concern over privacy don't always translate into privacy enhancing behaviours. Moreover, as privacy must be managed daily across multiple services, it is often done through

trade-offs in relation to factors such as time, context, and service (Sheehan 2002).

2.2 Ineffective Design

The current notice and choice model has a catalogue of problems (Calo 2012), they are long, incomprehensible privacy policies that users do not read or properly understand (McDonald and Cranor 2008). The legalistic and complex language acts as a barrier to comprehension and upfront policies place unnecessary demands on users at the point of sign-up. The combined effect is low levels of engagement with policies and poorly designed conditions for a user to determine control over how their data is collected and used. The lack of consideration companies give to the design and the user experience of privacy policies is a key factor in their poor design and the low levels of user engagement (Calo 2012; Schaub et al. 2015). Privacy notices are often 'bolted' on to a system, as opposed to being carefully integrated (Schaub et al. 2015:3), and they tend to receive less consideration than other areas of service design.

2.3 Timing & Lengthy, Complex Legal Text

Policies are strongly critiqued for presenting information in ways that disadvantage the everyday user. Policies are typically presented to a user at the point of sign-up when they require access to use a service. This is for legal compliance but leads to people ignoring notices and focusing on the immediate short-term benefits of signing up, rather than the implications or risks of sharing data in the long-term (Acquisti & Grossklags 2004). Policies imitate language in laws and regulations (Cate 2010), and obscure the information that users need to make decisions. The very nature of legal language is intentionally vague to ensure freedom in the potential use of collected data in the future. Moreover, as business practices with data become more complex, this will be mirrored in increasingly complex policy terms (Cate 2010). In 2012, 'Which' - a UK consumer watchdog, reported that PayPal's privacy notice, taken with its Terms of Service, came to a total word count of 36,275 – surpassing length of Shakespeare's Hamlet (at 30,066 words). To this point, McDonald and Cranor (2008) highlight that if an individual was to read the privacy policy at every website even once a year, it would amount to 244 hours of reading policies per year.

How policy information is presented has significant effects on how people respond to it (Schaub et al. 2015). It is not unsurprising that policy information presented in the ways described above, has led to disengagement and inadequate understanding of data practices, and ultimately people feeling detached and disenfranchised about their personal data. Policies that are lengthily and complex are highly impractical (McDonald and Cranor 2008) and solutions are urgently needed.

2.4 Informed Consent and Actionable Control

The notion of "informed" consent involves disclosure on behalf of one party and comprehension on the other. In the context of privacy policies, this amounts to company disclosure of data practices and an individual's accurate interpretation of what is being disclosed. For informed consent to have taken place, information must be presented in a way that can be *understood* and *acted upon* – which necessitates the provision of mechanisms to allow people to *exercise and execute* meaningful choices. That said, users are often denied access to a service unless they agree to terms of use and accept the terms laid out in privacy policies. A binary 'opt in/opt out, "take it or leave it" approach (Schwartz and Solove 2009) gives an illusion of choice. Long-winded disclosures of different aspects of data collection and use without parallel controls that allow people to opt-in or opt-out of specific data practices, fail to offer real control. Users that are required to agree to all the purposes set out by the organisation are denied the opportunity to make choices and negotiate terms with service providers. The mantra of 'user-control' permeates companies public-facing discourses when it comes to data, but this discourse does not always align with what services offer in terms of privacy provisions. Brandimarte et al. (2010) remind us that feelings of control can be counterproductive to privacy if they are not substantiated with effective controls for realising them. Informed consent relies on users having access to understandable choices and to controls that they can use that will effectively uphold their choices. As Cranor (2012:6) explains, notices 'have failed users to date and will continue to fail unless accompanied by usable mechanisms for exercising meaningful choice'.

2.5 The Design in Privacy by Design

Privacy by design and the development of new privacy enhancing technologies (PETS) address a variety of privacy risks. However, research into the visual and interaction design of policies has often come second to the technical implementations of designing privacy into systems (Calo 2012; Hartzog and Stutzman, 2013). To this point, Rubinstein and Good (2013) call for the 'design' to be put back into 'privacy by design'. Existing research includes (but is not restricted to): alternative layouts such as multi-layered approaches (Centre for Information Policy Leadership n.d; Pinnick 2011) which promote short, easy to read summaries to help users find information quickly and accurately; the nutrition label approach (See Kelly et al. 2009), which aims to standardise policies and make them easier to scan and compare; privacy warnings and summaries of benefits and risks to support decision-making in different service contexts; paraphrasing to increase time spent reading policy information (Waddel et al. 2016); and 'just-in-

time' transactional notices to notify users when a data practice becomes relevant (Schaub et al. 2015:5, ICO 2016). Other related design solutions include visceral forms of notice feedback (Calo 2012) and designing for privacy by obscurity (Hartzog and Stutzman, 2013) and 2015 saw the first systematic effort to map the design space of policies, identifying best practice and offering guidance to designers (Schaub et al. 2015) and the emergence of design tools to help support designers in the process of creating better solutions (Urquhart and Golembowski 2015).

2.6 Summary

The design of usable privacy notices and fairer models of data exchange for end users (see Mortier and Haddi 2014) remains a critical challenge. Several problems with privacy policies persist (1), many privacy policies still follow, or exhibit problems associated with the traditional, text-intensive format (2), policies continue to routinely disengage users and (3), data exchange models continue to be one-sided - protecting the interests of companies and service providers at the expense of balancing their interests with their obligations to end-users. The design space has not been fully exploited to help address these problems, and to date, existing research has not translated well into the type of coherent design guidance that is needed to support change in industry, and design practice (Rubinstein and Good 2013). HCI researchers are uniquely positioned to advance research and inform guidelines on designing more usable, effective, interactive and engaging privacy notices (Calo 2012; Lachello and Hong 2007; Hartzog and Stutzman 2013; Schaub et al. 2015). They can explore the untapped potential of the design space and evaluate and evidence the effectiveness of different approaches, techniques and solutions to advance current understanding, guidance and applied practice.

We identify 3 areas for HCI to focus on:

(1) Making data practices legible: With company data practices being complex and opaque, we must develop ways to support legibility, transparency,comprehension and engagement. A key challenge for HCI is designing to support different users in the process, acknowledging varying levels of interest, awareness, literacy, context, social usability requirements and available time.
(2) Providing meaningful controls: With increasing recognition that users need more effective control over personal data. A key challenge for HCI is to translate key principles and recommendations around choice and control into evidenced best practice, e.g. looking to determine the optimum amount of controls.
(3) Making data practices feel relevant to the user: With users feeling disengaged with company data practices and lengthy policies. A key challenge for HCI designers is to make data practices relevant, exploring practical and playful ways to engage and empower people in the process.

3. DESIGN RESEARCH: WORKSHOPS

Two industry workshops were conducted to explore usability barriers of an existing privacy policy and opportunities for improving policies with the goal to support users in managing their data practices. The first workshop included key service stakeholders from across the organisation and the second workshop consisted of service designers.

3.1 Workshop 1: Session with Stakeholders

Eight participants attended the first workshop - design researchers, computer scientists, software architects, and project leads. The workshop began with a brainstorming session in which participants were asked to discuss personal data and privacy. This led on to a more focused discussion about the nature of privacy policies - using the standard organisational policy as an example of current practice. Following this, the researchers introduced key usable privacy principles and principles for Human Data Interaction (see Mortier et al. 2014). These were used to stimulate discussion around how policies might be re-imagined. Specifically, three key high-level principles were identified to help stimulate ideas; (1) *Legibility:* making data practices transparent and comprehensible to the users (2) *Negotiability*: Providing the users with more choices pertaining to their data exchange and (3) *Agency*: Providing usable mechanisms for control of data exchange. Each principle was revealed to the group in succession and participants were asked to write down thoughts relating to the principle and ideas/techniques for achieving this. Following this, the group discussed the constraints and barriers that prevented them from applying these principles to privacy policies. To conclude, the group identified and prioritised key design challenges. The researchers recorded all the outputs from the workshop (ideas and research notes) and conducted a thematic analysis which involved coding the themes and ideas.

The stakeholders identified several areas to help improve the overall design of policies (1) Simplified language, consistent and common terminology, and the use of familiar conceptual models (2) Tailoring language to specific audiences e.g. accessible formats for people with access needs (3) Filtering of information to prioritise relevant information and summaries of policy areas (4) Easy to use controls/mechanisms for allowing people to negotiate consent and to allow for differentiated data access (5) Enhanced use of iconography and visuals to *show* rather than describe practices. Methods discussed for supporting this, included:

alternative visual designs, new control options, notifications, visualisations and alerts. At the end of the workshop, the stakeholders identified three design challenges. They believed addressing these were key to building more trusted data relationships with users:

(1) Designing for flexible, or personalised legibility to ensure policies are accessible to users with different levels of interest, expertise and needs
(2) Designing an optimum amount of choices that present the user with useful control but do not overwhelm them so they loose interest with the policy and process
(3) Designing so privacy decisions can be made before sampling the technology to help users understand the practical benefits and implications involved.

3.2 Workshop 2: Session with Designers

The second workshop consisted of 6 designers. They were given the design challenges identified by the stakeholders and challenged to come up with some possible solutions – using established design principles, and their creative expertise. The designers came up with several potential solutions to the challenges they had been set by their colleagues. The designers voted on their favourite ideas. The most popular 3 were as follows:

(1) *Curated data packages* allowing users to give different levels of consent for sharing data, covering different levels of granularity of choice for what types of data to share, and when, with the service provider.
(2) *Data visualisations* - showing examples of company data collection and data analytics, that 'preview' how a company will collect and use data - to improve on how this information is currently delivered e.g. in text-based form.
(3) *Multi-modal* policies were users can switch view to different presentational modes.

4. THE PROTOTYPE

A *clickable* prototype of a new policy design was created to 'probe' the design space of policies (see Hutchinson 2003). The prototype explored an alternative visual design and ways to afford the user's additional choices for managing their data and negotiating agreements with service providers. The final design was used as a research probe to facilitate discussion and reflection with users on the design space of policies. The new policy contained comparable information to the standard organisational policy, albeit displayed differently. The standard policy was a text-based policy written in full prose, with several hyperlinks to further information. The new design reduced the amount of text, improved navigation of the policy and made use of visuals and visualisations to help convey information about data practices.

4.1 Usable Privacy: Key Design Principles

Five key principles were identified:

(1) Transparency: making clear the data being collected and why
(2) Legibility: making data practices comprehensible to potential users
(3) Relevance: making data practices relevant to those it concerns in the context of service use
(4) Choice: providing understandable choices regarding access and use of data to help users make an informed decision
(5) Agency: providing visible controls that are easy to locate, understand and action - to support decision-making and setting preferences.

In addition, we took several measures to support ease of reading and navigation of the policy, improve on the levels of controls users have and introduce options for data negotiations with service providers – adopting guidance provided by the information Commissioners Office (see ICO 2017). For example, we adopted a simple style, aligned with in-house branding, the policy was written in a simple and engaging way for the audience– avoiding confusing terminology and legalistic language and we provided different levels of information to cater for different levels of interest. The design allowed individuals to positively opt in to data sharing, providing differentiated levels of controls as curated packages – supporting more granular control over specific aspects of data collection and use practices.

4.2 Design Elements

The design displays a circular menu which displays *clear simple data categories* which the user can click to explore related policy information (see figure 1).

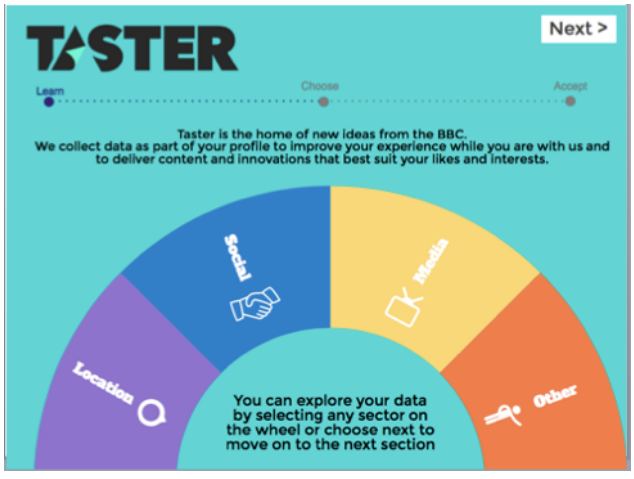

Figure 1. Landing UI, displaying the circular menu

The categories displayed on the menu were those that stakeholders and researchers identified as relevant to the user in the context of the service and the reorganisation of the policy information under these categories was fitting in the context of

use of the service. The wheel was intended to help the user explore and navigate policy sections and cater to specific interest's users might have in different aspects of data practices. The labels used were clear and simple to convey to the user the type of information contained within each category. The circular menu was prominently displayed to capture the user's attention, covering a large portion of the screen. It was designed to be aesthetically appealing and spark interest in the policy sections. In addition, it was consistent with the branding and overall service design to visually contextualise and reinforce the relationship between the policy and the service (ICO 2017; Schaub et al. 2015). Each category of data mapped to a different coloured segment to help the user identify and distinguish between data categories.

Information layers were designed into the policy. It followed guidance that notice layers should be hierarchal in structure; with the shortest notices capturing the main aspects of the data practice and subsequent layers revealing more information (Schaub et al 2015.). The circular menu was clickable, so the user could access more information about the different aspects of data practices relating to each category. It followed the information seeking principle of overview first, zoom, filter and 'details on demand'. This helped to accommodate any differences in levels of interest users might have in the policy (Shneiderman 1996). *Simple, accessible language* was used to explain the policy in each layer of information. Keywords and headers were provided at opportune points to help users identify relevant sections. Deciding what information should be included in the short notice was a crucial part of the design process as it needed to be concise but also accurate and informative. Top-level summaries were highly simplified but linked to summaries and then more detailed information if required. This layered approach aimed to avoid overwhelming the user with the entirety of the policy at once.

Our prototype included new *data visualisations* to provide alternative visual forms of displaying the policy information to users. These aimed to *show* the user how a company will use data rather than describe the process. This draws on Calo's (2012:5) 'visceral' forms of notice – the use of feedback mechanisms that leverage the experience of a service to facilitate the user's understanding of privacy within that specific context. He argues visceral forms of feedback have the potential to change a user's 'mental model' by showing users what is relevant to them, instead of long-winded descriptions of all the many potential possibilities. This design extended this idea of 'visceral feedback' to include 'behind the scene' visualisations of data processing connected to use of a service. The data visualisations acted as 'previews', designed to address the problem of asking users to sign up and agree to terms before using a service and with little knowledge of the service or the data it collects (Schaub et al. 2015). This preview technique was identified in the design-focused workshop, to give the user an insight into how the data a service collected from use of a service was used to make inferences about them as a user e.g. from their usage patterns. These had the specific goal of showing the user what types of inferences can be drawn from types of data collected, with a view to raising awareness and helping them make informed decisions about agreeing to share specific types of data. Pie charts were used to preview how the service collects data about time spent on the service, and aggregated watched history, showing time spent on different genres of content. In principle, this could be extended to include wider varieties of data types, data analytics and insights.

4.3 Data Exchange Options

We included a model of data exchange that introduced a new element of negotiation into the sign-up process. This was to explore how users felt this type of exchange model compared to the accept/decline model in the existing policy. We wanted to investigate if enabling the user to accept, decline *and negotiate* consent – would be welcomed by users, allowing them to negotiate use the service on more gradated terms. The design included options in the form of 3 data packages to give the user greater choice and decision-making power to determine what data they were happy to exchange for use of the service (see figure 2).

Figure 2. UI, displaying the 3 data packages

The use of packages drew inspiration from the 'freemium model' used in websites, a familiar conceptual model to many users. The reimagined design presented the user with a new model for data exchange. The user had the option of a '*simple starter package'* that requested basic information such as username and password but no interaction or behavioural data. This option still

allowed for use of the website. A *'customised package'* – this requested demographic information (e.g. name, age and gender) and behavioural data and offered the user a tailored service in return for personal programme recommendations. The final option was a '*personalised package'*, - this provided the user with highly granular control enabling them to choose specific data to exchange, using simple toggle buttons. Too many complex controls can make it difficult for people to articulate privacy preferences (McDonald and Cranor 2008) so for the personalised package we spent time trying to achieve the right balance with the controls, offering simple granular levels of control that would be sensible and effective in the context of the service provider's collection practices. The design focused on providing control over key areas of data collection and use that are *not currently afforded* in the existing policy terms. For each package, costs and benefits were clearly presented in bullet points. Information was given on the different kinds of data the service was requesting access to, the reasons for access, an overview of the costs and benefits of the data being exchanged and potential consequences. We were careful to convey the new options afforded in this policy in a clear way, making it clear to users the had options to choose and accept, decline or most importantly for this design - *negotiate degrees of consent*. Finally, a status bar was provided at the top of all pages to show the users where they were in the sign-up process. Pages also included back buttons for the user to undo the last action or move back to a previous page.

5. EVALUATING THE REIMAGINED POLICY

The reimagined design provided a research probe (Gaver 2001; Hutchinson et al. 2003). We presented this probe to potential users of the service. 15 participants were recruited for this study. We didn't want participants to explicitly focus on the policies, so they were not informed of our interest in the policies. They were invited to try out two interactive content pilots the service was developing, that required user data. These interactive pilots were used as a decoy so participants were not explicitly focused on the privacy policies but rather saw them as a way get to try the new content. This allowed us to investigate interactions with, and reactions to, the new policy. The probe also provided stimulus for a wider discussion about the design of privacy policies and provisions. Participants were recruited on the basis that they already used the service and had a general interest in interactive content. To ensure the participants were diverse, we recruited for a mix of ages (between 18 and 65), genders and socio-economic backgrounds. An agency was used to recruit the participants and they were offered a small incentive to come which would cover travel and time. The study took place in a replica living room environment. Participants thought they were there to preview and rate two new content pilots. They were informed that for each pilot they would need to first go through a simple sign-up process. One content pilot was preceded by the existing policy and the other by the reimagined policy. The order they saw the policies was randomised. The sign-up process was closely observed, interactions with both policies were logged, and reactions and any comments recorded. Once a participant had completed both pilots, the researchers revealed the explicit interest in the privacy policies over the content they had seen. The two privacy policies were presented back to the participants and the remainder of the session was focused on reflecting on the design of the policies, specifically comparing the existing and reimagined privacy policy. The researchers opted for a semi-structured interview and open questions. Opening questions included, for example, asking about the sign-up process of each content pilot, how much time they recalled spending on each policy, what policy information they could recall e.g. company data practices, and what type of consent they gave. Participants were asked about similarities and differences between the two sign-up processes, and to give descriptions of these differences and finally they were asked which policy they preferred and to give reasons. Walkthroughs of each policy followed to foster in-depth reflections on specific aspects of the policies, and discussion of key elements of the design. The interview allowed researchers to probe participants' attitudes about privacy and elicit reflections on the different designs. This provided an important platform for a wider discussion about the needs of users in relation to the design space of privacy policies. Participants' comprehension of the policy was probed but it was not comprehensively explored, as this was not the primary focus of this study. The data from the session was compiled, coded and thematically analysed.

5.1 Initial Reactions and Reflections

All 15 participants expressed a strong preference for the reimagined policy over the standard policy. Participants recognised spending more time on the reimagined policy and reported increased levels of interaction and engagement. Which was supported by the observation records and interaction logs. They descried being more interested and engaged in the new policy for reasons including: the simple layout, the use of colour, straightforward and inclusive language, gradual and progressive levels of detail, easy to understand categories, visible calls to action, intuitive navigation and the overall playful and inviting nature of the design. They self-reported a better understanding of company data practices with the reimagined policy and feeling more in-control, because of the choice they were given between different data sharing options.

5.2 Interest and Engagement

Participants described being more interested and engaged with the reimagined policy compared to the standard version, with all 15 stating a strong preference for the new design. The standard policy was described as dry, arduous, off-putting and generic and the process of agreeing to the terms as 'automatic'. Unsurprisingly, participants reported reading minimal information. P9 explained, *'I read a little, but then thought; this is boring'*. Participants reported making immediate judgements on whether to engage with the policy or not based on how much time and attention they anticipated was needed. P4 explained '*with the standard policy I make an immediate judgement, this is going to take up my time, so you just click accept to get on with it'*. In contrast, participants recognised spending more time on the alternative policy and giving it more attention. This aligned with the researchers' records and observations. As P2 explained, I spent more 'quality time' reading this one'. P7 recalled spending several minutes on the new design, 'I *spend more time on this one […] I took about 1-2 minutes. I didn't mind spending more time, I would normally be annoyed having to read all the terms but I didn't feel this way with this one*. Although participants reported spending more time reading and interacting with the policy – which could be considered undesirable - they did not begrudge the time they spent doing this. The extra time given to reading the new policy was felt to be less taxing and thought to be worth it, as P6 said*: I spent longer on it, but I felt clearer on it*. Many discussed key elements of the visual design as reasons why they spent time engaging with the policy. Reducing the amount of time people need to spend on reading and understanding polices is needed. If the process is more engaging, people may be willing to spend more time on policies. Participants frequently referenced visual elements when talking about key sections of the reimagined policy they liked. Specific aspects of the policy presentation that appealed to them included '*layout',* the '*data categories'* or '*groupings*' [P7], '*easy to scan information'*, [P1], nested information [P2], pictures, visualisations, and '*overall the user-friendly design'* [P15]. Participant 9 described the reimagined policy as '*a lot more open'* observing and appreciating that it *'was broken it down into readable sections, containing different levels of info'*. Overall, participants described their experience with the alternative policy as '*more enjoyable'* [P4] commenting that the design '*brought it* [the policy] *to life'* [P5]. As P14 summarises *'it was a more enjoyable experience, there was more clicking on things, it was more interactive - in a friendly way'.*

5.3. Accessible and Relevant Language

Participants likened the standard policy to standard service terms, which were described as a '*necessary evil'* [P3] to use a service. P1 explained that the standard policy '*looks like a legal document; it's off-putting, doesn't engage you at all, doesn't feel like it's part of the service. Its generic- it could have been for anything'*. Barriers to reading included the length and tone, the '*inaccessible'* and *'elite nature'* [P7] of the language, as well as the policy being *'dry'* [P5] '*off-putting'* [P15] and '*intimidating*' [P6] and full of '*legal language'* [P9] and '*jargonese*' [P4]. In contrast, the alternative policy was described as '*user friendly'* [P1], '*appealing*' [P10] and '*informative*' and appealing on the grounds of it being '*more conversational' in style* [P5]. Amounting to it being easier to understand overall. Participants appreciated the use of the accessible language. P7 liked that it was '*aimed at everyone rather than adults or elite audiences who know 'the language'*, describing it as more 'universally accessible', '*written 'in my language'* and [P5] who described it as '*more human-orientated rather than lawyer orientated'*. Participants liked being presented with information layers, with an overview that was '*simple, short, easy to use'* [P15] and text that made use of '*bullet points'* [P15], whilst also having access to more information on demand. As P1 noted: '*If you want to find out more, you can'*. Participant 15, self-identified as dyslexic she felt having less text and a more visual presentation was particularly helpful from a usability perspective. She wanted upfront options to render policies in different ways to suit different needs, noting this would have a positive impact on engagement with policies generally.

5.4 Information on Data Practices

When participants were asked what they could recall about the two policies, very few participants could recollect any details about the service providers' disclosure of data practices in the standard policy. Participants remarked that they could only make assumptions about was contained in the policy based on pre-existing knowledge or views held about the service provider, information about similar services and data agreements, or past experiences with policies. When P4 was asked about reading the standard policy he explained '*I almost ignored it all'*. When asked what he could recall he responded '*along the lines of we want access to all your data and you have no say and you can't sue us either. That's how I see most agreements'* [P4]. When asked if he understood what the service would do with his data he explained *'I'm probably unclear about how the data was used. I would like to think I would be clear but just based on experience, rather than what was written in the terms'* [P4]. In contrast, participants described reading and understanding information contained within the alternative policy and could recall more examples of company data practices. Most participants could discuss at least one aspect of the service's data practices and 14 out of 15

remembered the specific package they had selected and could provide a reasonable explanation for their decision to opt for that package over the other two, citing why their chosen package was preferred with regard to data sharing. Several could recall more detailed elements of the data associated with their chosen package. As a result, participants felt they had a better understanding of the terms in the reimagined policy. Talking about the reimagined policy P4, explained his choice for the personalised package *'I chose personalised package, because I think you should have more control over your data, and be able to change that at any time as well*' [….] Talking about the alternative design he went on to explain: '*I felt I knew more about how the service was using the data, it was easier to identify key bits, it was to the point.'* Discussions with participants suggested that they were more engaged with the new however further work is needed to comment on whether comprehension is improved through this, or other forms of interaction design.

5.5 Visible Choice and Increased Control

Participants appreciated the added control options afforded by the reimagined policy and could explain why they actively selected different data packages. Participants described selecting data sharing options that reflected their preferences for sharing data with the company. Participants that selected the basic package explained they preferred to share minimal data with a company to begin with - to allow them to access a service quickly and then revisit settings later. They expressed a desire to be able to edit preferences as they see fit. Participants who chose the personalised package - with the highest level of personalised control - reported a high interest in company data practices and a desire to understand how their data is used. They expressed wanting the capability to grant all, none, or partial consent. Regardless of the package selected, the added control was well received by all participants. P2's reaction captures this, '*on other websites, I've not had this level of choice before. I liked it!'* It is worth noting that one participant reported feeling overwhelmed by the level of control the alternative design provided. She felt she did not know enough about data practices and said she struggled to understand either policy and this reduced her confidence in any decisions she made. Whilst she articulated a preference for the reimagined design, she felt nervous that this policy made the company practices more obvious, which made her conscious of her 'inabilities' (sic) to make an informed decision. Participants appreciated how controls were presented in the new design, they specifically liked the *visibility* of controls and their high *prioritisation* in the design, which amounted to a clear call to action. Several participants observed that the lack of calls to action in the standard policy was an important reason for not interacting with it. Talking about the scroll feature in the standard policy P7 observed, '*I was not sure I could scroll down; it wasn't obvious. The design doesn't invite the user to do anything*' [P7]. In contrast, participants felt the controls in the new design were more readily perceived, and thus used. Its playful interactivity was described as 'sparking curiosity' leading to higher levels of interaction and engagement. As P14 explained, '*It was a more enjoyable experience, as there was more clicking on things, it was more interactive - in a fun and friendly way'*. Participants felt as though the added choice and options for control empowered them in the decision-making process as well as engendering a feeling of interest in the policy and control in the process. As P1 explained, that alternative design *'makes you happier in making a decision and in also using the service'.*

5.6 Data Visualisations and Previews

Participants liked seeing visualisations/previews of the ways companies use their data. Participants commented that they find this type of data interesting and it also has potential value on a personal level. They particularly liked seeing the specific breakdown of consumed content by variables such as genre and time spent watching different genres. This suggested granting access to data footprints in this context has several benefits. Discussing the data previews P7 noted, '*awareness of profiling is very limited generally, the relationship between data and what can be revealed'. Previews help make this clear from the offset.'* Participants made several further suggestions for techniques to improve their engagement with policies, these included, '*statements of data use annually or quarterly'* [P10] *personal data dashboards* [P7], *and nudges/reminders to check these* [P6], commenting that techniques like this would incentivise them, through the opportunity to gain personal insight.

6. DISCUSSION

The new design sparked a higher level of interest in the policy, a desire to spend more time finding out about the service's data practices and an interest in the new models for negotiating control.

6.1 Legibility and Engagement

Overall, the interviews show increased willingness by the participants to read policies when presented in an accessible, interactive and engaging way. The simple and relevant language was suggested to help with reading, processing, and recalling key aspects of the policy information and resulted in more time being spent on the policy. Whilst comprehension was not explicitly evaluated in this study, the interviews provided some evidence that the new design had helped participants' understanding of the policy information. Presenting information in a simple and visually engaging way - relevant in the context of the service - cultivated

interest and engagement in the policy and led to more time spent browsing and reading policy information (Waddel et al. 2016). We believe creative and interactive designs could help improve engagement in the policy process moving forward.

6.2 Visualisations of Data Practices

Previews of company data practices and analytics were well received. This sparked interest and discussion around what behavioural data was collected and the range of inferences that could be drawn about them from this. Users were interested in how this might work in other service contexts. Participants liked the idea of 'data dashboards' which could display this type of information. They liked the idea of seeing mocked up diagrams, charts, and analytic data about how a company uses data and how these techniques might be used to give real-time feedback on, and insight into, their use. This form of visual feedback was thought to be educational, personally illuminating, and more accessible than the existing method of text-based explanation, suggesting data visualisations/ previews in this context add value. We recommend further research into these 'preview' techniques.

6.3 Controls and Data Exchange

The controls in the reimagined design were well received. The added level of control, and the *visual prominence* of user control in the design was positively commented on. We introduced the package model to provide more flexibility in the sign-up process, allowing users to exchange data in different ways. Participants saw value in being able to negotiate in this way with service providers. They felt the new options and model for data exchange offered in the three packages, helped them make choices about what data to exchange for use of that service (e.g. little for basic functionality or more for a personalised service). These findings help to show the value of designing alternative ways to afford users choice and control in the policy space. We recommend research explores negotiable models of data exchange.

6.4 Trust

The reimagined design helped to foster stronger feelings of trust in the service. The findings suggest that engaging policies which appear to offer more usable information about data practices, help to improve active participation in the process and build trust in the organisation. This can help foster more productive long-term relationships between service providers and users. Exploring the design space of policies to improve engagement, e.g. through more appealing, interactive designs, presents an exciting opportunity for companies and public service providers to strengthen their relationships with users.

6.5 Limitations and Future Work

The strength of this work is the in-depth qualitative exploration of the policy design space of a company, using a reimagined policy as a probe that embodies how a service policy might otherwise be. The reactions and reflections of participants were in the context of research exploring a specific service and need to be understood in this context. Users have been shown to prioritise data differently when interacting with different services and sectors and trust can vary as a result (Bilogrevic and Ortlieb 2016). Familiarity with our service provider may have influenced responses. The reimaged policy was designed to be comparable to the existing policy but it was not identical as it was necessary to change some details to support the new features. In future, a more ecologically valid or longitudinal approach would have value as would examining comprehension more systematically. Future research might also consider focusing on expanding the range of interactive designs presented to users in different contexts and services, and increase the scale of the research.

7. CONCLUSIONS

This research probed the policy design space through a reimagined privacy policy of a UK media service provider. The findings highlight the opportunities for HCI to contribute to the design of usable privacy and support users in negotiating 'data-relationships' with service providers. The reimagined design generated higher levels of interest and interaction with the policy, which led to self-reported improvements in understanding company data practices and greater engagement in the privacy policy process. Gradated or negotiable models of consent and more visual forms of explanation – specifically the *'data use previews'* were thought to provide improvements to current policies. Whilst do not promote the policy design as a solution per se - to the service or more generally, we advocate the value of research and development into interactive, creative policy displays that can be customised for services - supported by user-centred evaluations. The paper argues the user experience of policies needs to be given greater consideration in the design process and should be evaluated to the same extent as other areas of service design. It also recommends that engagement should be included as an important metric when new designs are evaluated.

The limitations of the notice and choice model have led to its suitability being questioned in the long-term (Calo 2012; Cate 2010) but in the current circumstances we need research that aims to extend and advance the design space and develop evidence-based design guidance that industry and regulators can draw on. HCI researchers are uniquely positioned to advance understandings of the design space and develop the guidance for best practice that is currently needed.

Acknowledgements
We thank all the participants in the workshop and the study for their time and colleagues and reviewers who provided helpful comments on previous versions of this document.

9. REFERENCES

Acquisti, A. & Grossklags, J. (2004). Privacy attitudes and privacy behavior. Economics of Information Security, pp.165–178.

Brandimarte, L,. Aquisiti, A., Lowenstein, L. (2010). Misplaced confidences, Privacy and the control paradox. Ninth Annual Workshop on the Economics of Information Security (WEIS)

Barnes, S.B. (2006). A privacy paradox: Social Networking in the United States. First Monday. Retrieved:http://firstmonday.org/article/view/1394/1312_2 (Accessed 2.3.2017)

Bilogrevic, I, Ortleib, M. (2016). 'Attitudes Towards Data Combination and Sharing Across Services and Companies'. In Proceedings of the 2016 CHI Conference in Human Computing Systems Pages 5215-52

Calo, R. Against Notice Skepticism in Privacy (and Elsewhere). (2012). Notre Dame Law Review, 87 (3) 1027-1072. Retrieved: https://ndlrev.wordpress.com/volume-87-issue-3/(Accessed 28.2.2017)

Cate, FH (2010). 'The Limits of Notice and Choice', IEEE Security & Privacy, vol.8, no. 2, pp. 59-62, doi:10.1109/MSP.2010.8

Cavoukian, A. (2009). The 7 Foundational Principles Implementation and Mapping of Fair Information Practice. Retrieved from http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf (Accessed 28.2.2017)

Center for Information Policy Leadership, H. W. L. Multi-layered notices. Retrieved from https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/ten_steps_to_develop_a_multilayered_privacy_notice__white_paper_march_2007_.pdf (Accessed 4.3.2017)

Cranor, F,L. (2012). Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. Journal on Telecommunications and High Technology Law 10(2), 2012, 273-307.

European Parliament and Council (2002). Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. Official Journal of the European Communities, (L201) 2002. http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_en.pdf. (Retrieved March 3. 2017)

European Parliament and Council. (1995). Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, (L 281/31). http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (Retrieved March 3. 2017)

Federal Trade Commission (2012). Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policy Makers. Retrieved from http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. Retrieved 28.2.2017

Gaver, W. (2001). Cultural (s- Probing People for Design Inspiration. SIGCHI. DK.

Hartzog, W., Stutzman, F. (2013). Obscurity by Design. Washington Law Review, 88, 385-418.

Hutchinson, H. Mackay, W, E., Westerlund, B (2003). Technology probes: inspiring design for and with families. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '03: 17–24. http://doi.org/10.1145/611.642616

Iachello G, Hong H .(2007). End-User Privacy in Human–Computer Interaction. Foundations and Trends in Human–Computer Interaction Volume 1 (1).

Information Commissioners Office (ICO 2017). Privacy Notice. https://ico.org.uk/global/privacy-notice/ Retrieved March 3. 2017.

Jenson, C. Potts, C(2004). Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. CHI'04, Vienna, Austria

Kelley, Patrick Gage, et al.(2009) A nutrition label for privacy. Proceedings of the 5th Symposium on Usable Privacy and Security. ACM,

Lugar, E Urquhart, L. Golembowski, M. (2015) Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process. In Proceedings of the 33rd Annual ACM Conference on Human Computer Factors in Computer Systems Pages 457-466.

Information Commissioners Office (ICO 2017b). Privacy Policies, Transparency and Control. https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control Retrieved March 3. 2017.

McDonald, AM. Cranor, LF. (2008). The cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 4(3) 40-565

Mortier, Richard and Haddadi, Hamed and Henderson, Tristan and McAuley, Derek and Crowcroft, Jon (2014) Human-Data Interaction:

The Human Face of the Data-Driven Society http://ssrn.com/abstract=2508051

Ramirez, E (2012). Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission. Federal Trade Commission Retrieved:https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf Retrieved 1.2.2017

Paris (2012). Online T&Cs longer than Shakespeare plays – who reads them? Which. Retrieved from: https://conversation.which.co.uk/technology/length-of-website-terms-and-conditions/(Accessed 3.3.2017)

Pinnick, T. (2011). Layered Policy Design | TRUSTe. Retrieved from: http://www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/ [Accessed 1.11. 2017].

Rubinstein, S., Good, N. (2013). Privacy by Design: A counterfactual analysis of Google and Facebook Privacy Incidents. Berkeley Technology Law Journal. Article 6. Vol 28 (2)

Solve (2012). Understanding Privacy. Harvard Univeristy Press Massachusettes. London. England

Shneiderman, B. (1996). The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations. In Proceedings of the IEEE Symposium on Visual Languages, pages 336-343, Washington. IEEE Computer Society Press http://citeseer.ist.psu.edu/409647.html

Schaub F, Balebako, R., Durity, AL,. Cranor, LF (2015). A Design Space for Effective Privacy Notices. Symposium on Usable Privacy and Security. Ottowa, Canada

Sheehan, K.B. 2002. Toward a Typology of Internet Users and Online Privacy Concerns. The Information Society, Vol 18 (1)

Schwartz, PM & Solove D. (2009) Notice & Choice. In The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children

Waddel TF, Auriemma, JR., Sundar, S. (2016). Make it Simple, or Force Users to Read? Paraphrased Design Improves Comprehension of End User License Agreements. CHI ’16. San Jose, USA.

Westin, AF.(1967). Privacy and Freedom, New York: Atheneum