IADIS International Journal on WWW/Internet
Vol. 13, No. 2, pp. 1-16
ISSN: 1645-7641

SCARED OR NAÏVE? AN EXPLORATORY STUDY ON USERS PERCEPTIONS OF ONLINE PRIVACY DISCLOSURES

Helia Marreiros[a] , Richard Gomer[b] , Michael Vlassopoulos[a], Mirco Tonin[c] and m.c. schraefel[b]

[a] *University of Southampton, Department of Economics, School of Social Sciences, SO17 1BJ, Southampton, UK*

[b] *University of Southampton, Electronics and Computer Sciences, SO17 1BJ, Southampton, UK*

[c] *Free University of Bozen-Bolzano, Faculty of Economics and Management, 39100, Bolzano, Italy*

ABSTRACT

Online service providers offer “free” services in exchange for the personal data of its users. In the last few years there has been an increase of online industry regulations requiring service providers, such as websites and app developers, to disclosure the ways in which they collect, process and use the personal data of service users. These “privacy disclosures,” such as the privacy policy, the cookie notice and, on smart phones, the app permission request, are designed with the purpose of informing users and empowering them to control their privacy. The interaction problems with these different types of disclosure are relatively well understood – habituation, inattention and cognitive biases undermine the extent to which user consent is truly informed. Users understanding of the actual content of these disclosures, and their feelings toward it, are less well understood, though. In this paper we report the results of a mixed-method exploratory study of the privacy disclosures and compare their relative merits as a starting point for the development of more meaningful consent interactions. First, we conducted a focus group study, with 21 students from the University of Southampton, to understand behavior and privacy concerns of Millenials (those born between 1982 and 2004) in response to the these three most common types of privacy disclosure. Second, we conducted an online survey, with 100 students from the University of Southampton, to study perception and feelings towards the content of the privacy disclosures. We identify three key findings. Firstly, we find heterogeneity of user perceptions and attitudes to privacy disclosures in both studies. The results of the focus groups suggests three types of users: the *scared* and worried about their online privacy, who think there is an option out; the *naïve*, who do not understand how their personal data is collected and processed by the online service providers; and the *meh*, who understand the tradeoff but are not worried about their privacy. Secondly, we find limited ability of users to infer data processing outputs and risks based on technical explanations of particular practices, suggestions of a naïve model of “cost justification” rather cost-benefit analysis by users. Finally, we show evidence of the possibility that consent interactions are valuable in themselves as a mean to improve user perceptions of a service.

KEYWORDS

Privacy; Consent; Cookies; Apps

1. INTRODUCTION

The extent to which users are in control of their personal data is a hot topic among policy makers, legislators, researchers and users themselves. In the European Union, the United States of America and beyond, organizations commonly explain their data processing practices to consumers via detailed privacy policies. Furthermore, legislation on both sides of the Atlantic requires user consent to specific data uses either in specific scenarios (such as granting permission to be sent marketing emails) or as a general data protection principle.

The extent to which users' consent can be said to be informed, or *meaningful*, is intuitively dependent on the quality of the content of these “privacy disclosures” in terms of how well they help users to understand the processing that their personal data will be subject to, how they can control that processing and how the processing might impact them.

In this paper we present the results of a mixed-methods exploratory study into the understanding, behavior and privacy concerns of Millenials (those born between 1982 and 2004 (Howe & Strauss, 2000)) in response to three common types of privacy disclosure: 1) The privacy policy, itself; 2) Cookie Notices: small notices that are displayed on websites; and 3) App Permission Requests.

We use the qualitative and quantitative insights from these investigations to compare these three types of privacy disclosure and to suggest how future disclosures might be designed. First we report the results of four focus groups, showing the heterogeneity of preferences and concerns toward privacy disclosures. We also show that participants typically view these disclosures negatively unless they are able to understand why a particular type of processing is taking place, and also that they consider other aspects beyond this, such as whether they are being treated fairly in the way that the choice is presented to them. Second, we report the results of two online surveys.

We show that in both surveys, the first about privacy policies and app permission requests and the second about cookie notices, there is significant heterogeneity in users’ perceptions and feelings towards statements made by service providers and manufacturers regarding the use of, or access to, personal data. In the first survey we show that users consider that some privacy policies reflect a positive attitude of the service provider towards their users (such as those referencing the *protection* of privacy), others a negative attitude (such as those informing users about how their personal data could be *shared*), while others perceived as more neutral (often those referring to technical details). We also show that most users perceive app permission negatively and are willing to pay a small amount to protect their privacy. This result seems to be driven primarily by skepticism over the legitimacy of many permission requests given the purpose for which the user installed the app. In the second survey, we show that cookie notices that refer to users’ privacy and provide more detailed explanation are perceived more positively than those that merely state the presence and use of cookies.

The contribution of this work is to better understand the process by which users make sense of the privacy information with which they are provided. Existing literature, (egKelley et al., 2009), confirms the lived experience of most web users, ie that users do *not* read privacy policies. However, conveying information to users – in some form – must, by definition, form part of any future consent mechanisms and so understanding how such information is understood by users provides, as we shall discuss later, important insights into the development of more meaningful consent interactions in the future.

The remainder of this paper is organized as follows. In section 2 we start with a discussion of relevant issues in meaningful consent and give a brief description of the three types of privacy disclosure that are considered in this work. In section 3 we present the study methodology and procedures. Section 4 presents the results of the exploratory investigation. Finally, we summarize our findings and conclude in Section 5.

2. BACKGROUND

Regulators and policy makers, at least within Europe, are increasingly using user consent as a mean of empowering data subjects to control the processing of their personal data. This is evident in the 2009 ePrivacy directive (Anon, 2009) as well as the upcoming General Data Protection Regulations (GDPR). However, as anyone who has read a privacy policy or experienced one of the UK's “cookie notices” can vouch, the consent mechanisms that arise from these regulations have not, to date, led to the routine collection of what we might consider “meaningful” consent from data subjects and seem, for the most part, more concerned with the creation of a legal fiction rather than genuine empowerment of data subjects.

2.1 Consent

Existing work on consent typically considers the requirements for “informed” consent, and although we purposely use the term meaningful to distance ourselves from existing legal assumptions about consent, work on informed consent is a principle that influences our work.

Informed consent involves two broad components: information (in which a person is provided with information) and assent (in which they signal that they agree to the request that is being made). In offline media this process could take the form of reading and signing a physical form, and on a conventional computing device it often involves reading a notice and clicking a button.

Friedman et al. (2002)formulate informed consent as consisting of six key components: Disclosure (providing adequate information), Comprehension (the individual having sufficient understanding of the provided information), Voluntariness (the ability for the individual to reasonably resist participation), Competence (the individual possessing the requisite mental, emotional and physical capabilities), Agreement (a reasonably clear opportunity to accept or decline participation) and Minimal Distraction (the consent process itself not being so overwhelming as to cause the individual to disengage from the process). Of these six, Disclosure, Comprehension and Competence are the most highly dependent on the content that is provided to the user, while voluntariness, agreement and minimal distraction are largely properties of the broader design and choice context.

In this work we focus primarily on the content of the privacy disclosures and how users comprehend this information. However, numerous behavioral biases and cognitive shortcuts, such as decision fatigue, habituation or aversion to irrelevant or incomprehensible legal information (Kahneman & Tversky, 1984; Böhme & Köpsell, 2010), make meaningful and informed consent problematic for human beings. While the content of a disclosure is a necessary component of meaningful consent, we do not claim that it is sufficient in itself, and issues such as presentation and interaction still need to be considered from a behavioral point of view.

2.2 Cookies and the ePrivacy Directive

Cookie notices are commonly displayed in some European Union member states, as a result of the EU's revised ePrivacy directive. They are designed to fulfill the directive’s requirement that service providers obtain user consent before data is stored on, or retrieved from, a user's computing device.

Browser cookies are a technical mechanism for maintaining state between HTTP requests. Although they support numerous online interactions – including, for instance, the ubiquitous “shopping basket” – their use has evolved to support data sharing both within and across sites. So-called “third parties”, such as advertising or analytics companies, may use a single persistent cookie to track users as they browse through affiliated websites (Mayer & Mitchell, 2012) for the purposes of understanding user interests, demographics or other profile information, often forming highly interconnected and pervasive networks (Gomer et al., 2013). It is as a result of concerns about the use of cookies for purposes such as third party tracking, and the impact that this has on citizens' privacy, that the European Union introduced the consent requirement into the 2009 revisions of the e-Privacy Directive (Anon, 2009).

In February 2015, a joint survey of popular websites by the European data protection regulators (ARTICLE 29 DATA PROTECTION WORKING PARTY 2015) found that many operators now provide some disclosure of cookie use, but that only 16% of sites provided granular controls over which cookies are used.

2.3 Privacy Policies

Privacy policies are a legal requirement in many jurisdictions. They are typically required to contain information about the types of data that an organization collects and the ways that it may be processed (eg.Kelley et al., 2012).

There are difficulties in creating privacy policies that are concise enough for users to read but which convey all the information that is required for users to make informed decisions. Previous research has aimed to make privacy policies more readable (Mcdonald et al., 2009; Kelley et al., 2009) or standardized (Cradock et al., 2015). Other research shows that, when users feel that they have understood a privacy policy, they are more likely to trust the web site to which it applies (Ermakova et al., 2014).

In this paper we study how users feel when the privacy policies of online service providers, such as Facebook and Google, are highlighted and what their understanding is of those privacy policies.

2.4 App Permissions

The use of ‘apps’ on smart devices such as mobile phones or tablets potentially creates privacy concerns for users. These apps may access, process and transmit personal data that is stored on the device (such as photos or contact information) or which is available through the various sensors embedded into the devices (for instance location, or even, in the case of some devices, physiological data such as heart rate).

On the Android platform (and others) the user is informed and must explicitly opt to continue installation of an app if it requires access to personal data, such as their address book or location.In Android M, this process is made more granular and the user must make a decision about each permission, the first time that a permission is required by the app.

Previous research has shown that app users are often unaware of the extent to which apps can access personal data(Kelley et al. 2012; Liccardi et al. 2014)and the potential privacy and security issues that this access can cause.

Despite the presence of this supposedly informing feature, many users still find app behavior 'creepy' (Shklovski et al. 2014) which suggests that it is not succeeding in fully reassuring or empowering app users.

3. STUDY METHODOLOGY

3.1 Focus Group

The first part of our study took the form of focus groups in which we led a discussion among four groups of "millennial" students – a mix of undergraduates and postgraduates - about their perceptions, understanding, and concerns relating to the three types of privacy disclosure: privacy policies, cookie notices, and app permission requests. Each of the four groups had between 4 and 5 members and lasted for about one hour. In total 21 students participated in the study.

The aim of these groups was to glean a qualitative understanding of the factors that seem to influence the participants' understandings and opinions of the different disclosures. Moreover, we aimed to understand what type of privacy policies, cookies notices and app permission requests users considered to reflect a positive, negative or neutral attitude of the online service provider or app developer towards their users. This was crucial to the choice of the privacy disclosures in the second study, the online survey.

Participants for the focus groups were recruited primarily from interns and postgraduates at the University of Southampton by means of mailing lists and personal invitation, although some participants were drawn from other departments. Participants were provided with an information sheet about the purpose of the study and what to expect during the session.

Participants were seated around a table with two of the investigators. The sessions were structured through the use of a set of slides that were projected on to a screen. The slides had four sections:

1: A series of statements taken from online privacy policies. We asked participants if they thought the statements showed a positive, negative or neutral attitude of the service provider towards their users, and to explain why.

2: Screenshots of some cookie consent notices from UK websites. We asked participants to explain the reasons that they thought the website was displaying the notice, what the notice meant, what the website would do and what they thought other parts of the notice (including phrases such as "improve your experience") might mean.

3: A series of statements taken from the Android app permission descriptions, such as "This app would like permission to... access your contacts". We asked them to explain what they thought each permission meant, and their feelings towards apps that request it.

4: Two exercises in which participants were asked to imagine what information a) Facebook and b) a behavioral advertising company, like DoubleClick, might know about them.

At the end of the focus group participants were asked to rate 25 statements taken from Facebook and Google's privacy policies. In the two first focus groups participants completed this task on paper at the end of the session, in the other two groups participants were directed to fill it out online.

3.2 Online Survey

The second part of the study took the form of an online survey. 99 "millennial" participants were recruited primarily from the University of Southampton via student groups on Facebook.

66 participants were first shown 14 statements taken from Facebook and Google's privacy policies, and 10 app permissions taken from Android smart phones. They were asked to indicate whether they felt each one showed a positive, negative or neutral attitude of the service or app developer towards their users(see table 1 and table 2in appendix A).At the end of the survey they were presented with a hypothetical scenario in which they were asked to imagine that they were purchasing a new app. They were then asked to reveal how much they would be willing to pay (from £0 to £5) to use the app *without* giving it permission to access the data stored in their phone.

> *"You are about to purchase a single-player game for your mobile phone in the app store. There are many versions of this game available depending on the permissions you give to the app, such as its ability to see your location or to read your texts. You are able to turn off all the permissions and the game will still function. However, this will cost you £5. If you give all the permissions it asks for, the game is for free. You can choose which permissions you do not want your app to have.*
>
> *Please specify how much you are willing to pay to deny the following permissions to the app, on a scale from £0 to £5:" (*see table 3 in Appendix A for a description of all the permission requests).

The 14 privacy policy statements were selected from a larger initial set of 25, based on ratings provided by participants from the focus groups. Our inclusion criterion was that the statements had been rated as positive or negative by more than 55% of the initial focus group participants and neutral by more than 45% of those groups (as none reached the 55% level of consensus for neutrality).The app permission requests were selected from the most widely used apps (worldwide) in the Google Play store, such as Facebook, WhatsApp and a selection of games.

We conducted a second survey in which 33 participants were shown seven cookies notices and asked to rank whether they felt each one was positive, negative or neutral (see table 4 in appendix A). We also asked participants to rate, overall, whether they felt the presence of cookie notices on websites was in itself positive, negative or neutral and whether they recalled seeing such notices previously.

4. RESULTS

4.1 Focus Groups

In the focus group study we found that the majority of students were familiar with cookie notices, privacy policies and app permissions. However, we also found a significant degree of misunderstanding about what the content of each disclosure meant and a very mixed set of concerns relating to specific pieces of content found in each. Results are discussed for each type of disclosure, along with general findings that are common to all.

4.2 Cookie Notices

Almost all of the participants recalled seeing cookie notices, although many were quick to add that they rarely read them and usually just clicked agree or ignored them. When asked what they thought the notices meant, participants were often unable to suggest how cookies could fulfill a purpose such as “make this website better” or “improve your experience”. Typically, though, they interpreted this as personalization. A few expressed that the intent was to collect analytics through which the website could be improved in general rather than made to work better specifically for them, but those participants were in a minority.

A few participants explained that cookies could be used to access browsing history, others thought that cookies stored information about demographics, but were unsure how this information was obtained.

Some participants felt it was unfair to declare the use of cookies but provide no means to opt-out. In the words of one participant, it is “undemocratic” to provide no means to use a website without being able to reject the cookies. This sentiment does not necessarily seem to be driven by a particular concern over the use of cookies in general, rather a response to the lack of choice in itself.

Many participants were reassured by the statement that the cookies would not interfere with their privacy, but some were critical of this statement. They expressed doubt that remembering things about their visit could be done in a way that did not interfere with their privacy and commented on the subjective nature of what constitutes privacy.The vast majority of participants did not realise that Facebook also has access to partial browsing history gleaned through their “share” and “like” widgets.

4.3 Privacy Statements

Participants were mixed in their responses to the individual privacy statements. Statements that referred to “protecting” privacy or to *not* sharing data were perceived positively.

They were generally negative towards the idea of Google or Facebook sharing data with third-parties, nevertheless, most participants suggested that they trusted that those companies would not do anything to harm them.

Many participants mentioned the perceived lack of choice and a contagion effect – for instance commenting “there is no option if I want to use Facebook or Google, as everybody is using it”.Given the wide range of services provided by Facebook and Google and their many subsidiary companies and partners, participants were unsure what the “family of companies” that constitute Facebook contained and so did not understand which companies their data might be shared with. One participant interpreted this statement very broadly, as including all companies with a Facebook page.

There was also a negative consensus about the idea of processing their personal data in foreign countries. This was seen as unnecessary and potentially risky, some participants commented that they might have less legal protection if their data was transferred abroad.

When we asked participants to comment on purely technical statements, such as explanations of cookies and pixels, they were generally less negative but felt that the purpose of their use was important.

4.3.1 App Permissions

Apps that ask for permission to access features or data on smart phones were perceived negatively, but this seems to be contextual. Participants said they viewed permission requests more positively when they understand why the permission has been requested and perceive that behavior as a legitimate function of the app. Some participants expressed resentment at the lack of choice they have, such as the inability to reject individual permissions.

Participants had differing interpretations of what the permissions meant in practice. For instance, the "full network access" permission was viewed negatively because participants felt this implied that the app would be "browsing the web" in the background.

4.3.2 General Findings

In all three scenarios – privacy policies, cookie notices and app permissions – participants seemed to take into account the purpose of the request when articulating their assessment. Cookies that ostensibly "improve" experience are seen more positively. Apps that request permissions were seen generally negatively, except when participants felt that the permission was justified given the purpose of the app. Privacy policy statements that refer to data or/and privacy protection were received more positively than those that indicate that their personal data would be shared with third parties or processed in other countries different from the one they lived on.

Cultural context, or specific privacy concerns, seems to be taken into account by participants. This was particularly common among our foreign participants who often related it to the cultural context of their home countries. For instance, a Turkish participant spoke of how they felt they had less freedom to criticize the government; a Mexican participant linked posting photos of his dog to the risk of it being stolen for ransom and another participant spoke of the different risks that male and female internet users might face because of the cultural expectations around gender in his home country.

At the end of the focus groups, and following a debrief session during which we answered any questions that participants had about the issues we had touched on, most of the participants admitted to feeling more concerned about their privacy than before taking part in the focus group. This sentiment was not universal, though. Some of the participants expressed that they had learned new things about the mechanisms or extent of, for instance, third party tracking, but still did not feel it was a problem to them personally.

This focus group study had 3 main outcomes. First it helped us to map the heterogeneity of the "millennial" generations. Broadly, we found that most participants could be categorized as one of three stereotypes: The "Meh", those who reveal that they don't care about their privacy or how the online services providers are using theirs and others personal data; the "Scared," who realize the risks of sharing personal information, but felt they don't have an option out;

and the “Naïve,” who don’t have a clue of what is happening online, just want to use the services and trust that the companies will not do anything to harm them or sell their personal data. Second, it allowed us to observe the reactions of participants as they became more aware of data collections and processing practices and (in many cases) decided to be more protective of their data.At the end of the focus groups, and following a debrief session, most of the participants admitted to feeling more concerned about their privacy than before taking part in the focus group. Finally, it helped us to choose the privacy policy statements, app permission requests and cookie notices to be used in the online surveys.

4.4 Online survey study

4.4.1 Privacy Policies

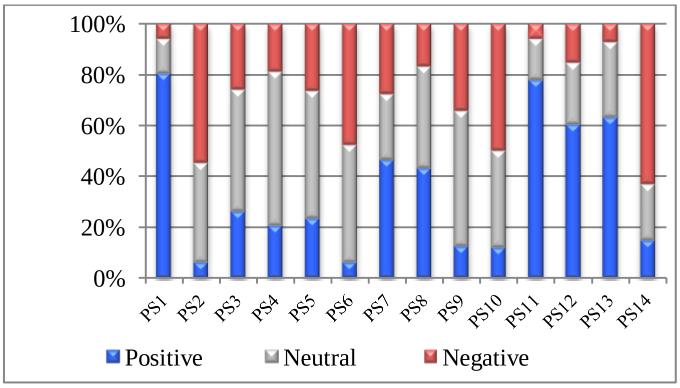

Figure 1. Privacy policy ratings

Figure 1 shows the percentage of participants that ranked each of the privacy policy statements as positive, neutral or negative (see table 1 in appendix A for a description of all the privacy policies’ statements). We observe a large degree of heterogeneity in how participants perceived the privacy policy statements. However, there are some trends in how different types of statement were rated. For example, statements like PS1, PS12 and PS13 refer to data protection, privacy concerns and trust, and the general population of this study considers those to be positive. On the other hand statements that suggest data is going to be collected and shared, for example PS2, PS10 and PS14, are considered to be negative. Statements about cookies – such as their definition and usage - are normally considered to be neutral; for instance PS3, PS4 and PS9.

These results are consistent with those found in the focus groups and indicate that when users do read the privacy policies, they do understand them to some extent, considering positively those that refer to the protection of their data and to personalization and negatively those that indicate data collection and sharing.

4.4.2 App Permission Requests

Figure 2 shows how participants perceive app permission requests. We can observe that a majority of those permissions requests were considered negative in a 7-scale “strongly negative to “strongly positive.”

Permission requests to access the user's location (PER4), read their calendar (PER9) or grant full Internet access (PER5) were rated as neutral. However permission about contacts (PER1), accessing or sending SMSs (PER3), modify stored files (PER6) or taking photographs (PER8) were considered extremely negative by the majority of the participants (see table 2 in appendix A for a description of all the permission requests).

Figure 3 shows the willingness to pay for privacy. We can see that participants were willing to pay between £1.50 and £2.75 to protect their privacy, denying permissions to the app developer. Read SMS (AP6), track browser history (AP11)and take pictures with the camera (AP12) were the permissions that participants were most willing to pay to deny. Users are less willing to pay to deny permission requests related to their location (AP1-AP4) (see table 3 in Appendix A for a description of all the permission requests).

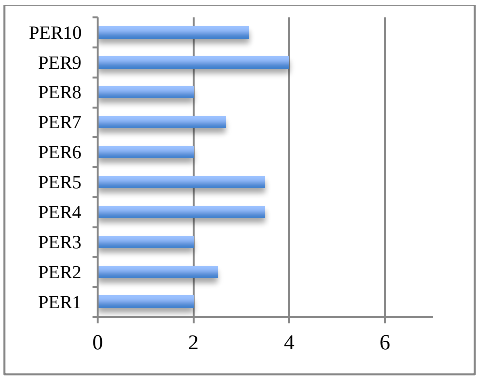

Figure 2. Apps permissions' rating 7 likert-scale

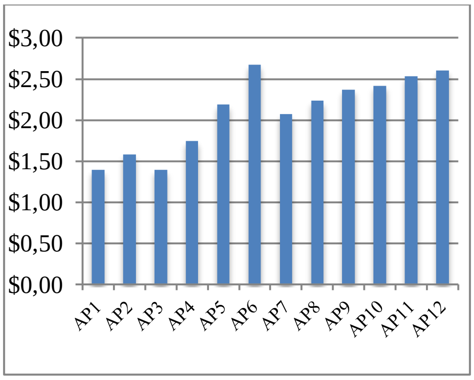

Figure 3. Willingness to pay to denyapp's permission requests - scenario

The users' perception of app permission requests as positive or negative is correlated with their willingness to pay. For example, participants rated as highly negative permission requests related to reading and editing SMS's (PER3), and were willing to pay £2.75 to deny this permission to the app developer (AP6). We can also see this correlation in relation to reading contact data from the users address book - between PER1 and AP8. On the other hand, participants considered permission requests related to location as negative, but not so negatively as those previously mentioned, and were willing to pay only around £1.50 to deny that permission.

Users seem to be more reluctant in accepting permission requests that involve data from third parties (such as friends or contacts) than those only involving their own data, such as location and calendar (PER9). We can see that they perceive the calendar request neutrally in the rating, but are willing to pay to protect the calendar when it involves friends and co-workers (AP10).

4.4.3 Cookie Notices

In the second survey, when asked if they thought that the use of cookie notifications in general is positive, negative, or a neutral, 63 percent of the participants answered that they were neutral towards it and only 9 percent indicated that they considered the practice to be negative. (see table 4 in appendix A for a description of all the cookie notices).

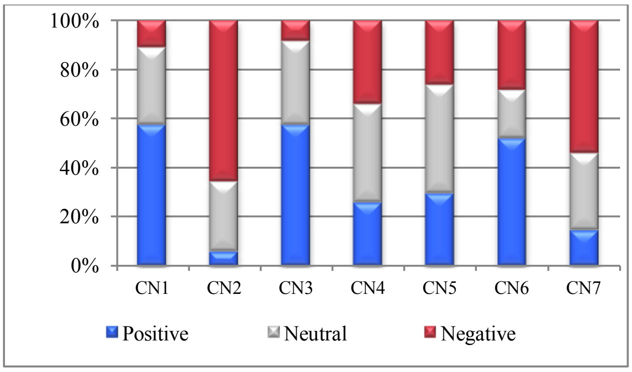

Figure 4. Cookie notice rating

Nevertheless, as seen in figure 4, we see significant variation in how different notices are rated. Cookie notices that inform the user that by continuing to use the site they are consenting to the use of cookies, without further explanation, as is the case of cookie notice (CN2 and CN7) are perceived as negative.

5. DISCUSSION AND IMPLICATIONS FOR DESIGN

The results presented in this work indicate that the different forms of privacy disclosure have different impacts on user understanding and hence on the meaningfulness of the consent that the users give. Our key findings are in four areas: Heterogeneity & Personal Context; Limited User Inference; Cost Justification and The Value of Consent.

*Heterogeneity & Personal Context:*We observe significant heterogeneity between participants with regard to which content is considered positive, negative and neutral. This seems to be partly the result of different beliefs about what the statements mean in practice, perceptions of the legitimacy of the processing that is disclosed and personal sensitivity to privacy concerns in general.

The qualitative findings from the focus groups indicate that privacy attitudes are very diverse and depend on personal concerns and context. Users link the information that they're provided with to a diverse range of values and their own situation. This context includes physical location, culture and specific privacy concerns such as being part of a particular social group.

Assisting users in relating data-handling practices to their own contextual concerns should be a goal for meaningful consent interactions,although it is unclear exactly what types of interaction might help with this. There is, perhaps, an education aspect in helping users to predict the likely impact of a given practice, but this should not absolve service providers themselves of their responsibility for fostering user understanding.

Limited User Inference: Related to personal context, there seems to be a general inability among users to infer the possible uses or effects of a piece of technology, or to infer the impact on their own privacy from a particular practice or data collection purpose. For instance, many users are unable to infer that the use of cookies allows their web browsing history to be tracked by third parties, and further are unable to infer that this tracking allows information about their demographics or interests to be inferred by those third parties.

This raises the question of how explanations should be framed. At present, most of the cookie notices are framed in purely technical notions - "we use cookies" - and provide very little information about the actual uses to which those cookies will be put. For instance, none of the cookie notices we observed in the course of preparing the focus group materials explained that cookies would be used to target advertisements or draw inferences about the user, although this was clearly the case on many of the websites we visited. App permissions are also largely technical. They provide granular control over what data or features an app can access, but provide no information about what purpose that access will be put to. Privacy policies contain a mix of narratives, covering both purpose and technology. However, statements about technology are often hard to understand and are often accompanied by fairly general statements about purpose that make contextualisation difficult.

*Cost Justification:*Despite frequent claims that users make cost-benefit judgments when using online services, and that the use of online services reveals a preference for services over privacy, we find little evidence of that through the focus groups. The lack of user understanding and inability to articulate the link between described practices and personal privacy concerns itself seems to preclude any meaningful cost estimation. However, we did observe that many participants engage in a form of "cost justification", particularly with regard to app permissions.

This conclusion, which implies that most users take a negative-by-default view of data collection or sharing seems to be supported by the finding that privacy policies that indicate that personal data is being collected or shared are considered negative by the majority of the participants, whereas those indicating that personal data is going to be protected and not shared are perceived positively.

*The Value of Consent:*Many participants, in the case of app permission requests and cookie notices, feel that a notice with no real choice over the use of cookies or which permissions are allowed is in itself a negative thing. This does not necessarily seem to be based on specific concerns but instead seems to reflect a preference for choice itself. This is reflected in both the qualitative focus group data as well as the quantitative data from the cookie survey. Cookie notices 2, 4, 5 and 7 – the least positively rated notices – are framed as an ultimatum using language such as "we assume." This is interesting, as it suggests that consent interactions that provide meaningful choice to users improve the user's perception of the relevant app or service, and complements the earlier research that shows improved trust as a result of more readable privacy policies (Ermakova et al. 2014).

This finding suggests that users evaluate consent interactions with regard to instrumental as well as terminal values. That is to say that they care about the way in which choices and information about data processing are provided to them, as well as just the options that they have. The implication is that meaningful consent interactions may provide value to service providers beyond just legal compliance, acting as a means to improve user trust in a service.

6. CONCLUSION

The results and challenges presented here outline some of the challenges for designers and providers of online services that rely on consent from users. They provide some guidance to policy makers about the potential pitfalls of consent – such as framing explanations in technical terms that, while truthful, do not appear to support user understanding.

As well as identifying some particular challenges that those interested in consent must overcome, we also find that consent in itself seems to be valued by users and that providing consent may have intrinsic value beyond merely legal compliance.We show that users typically view information disclosures negatively unless they are able to understand why a particular type of processing is taking place, and that they consider other aspects beyond this, such as whether they are being treated fairly and if the service provider or app developor is trustworthy.

Future research could look at the relationship between trust on the website or app developer and evaluation of content of privacy polices and app permissions requests

In future work, we intend to address each of the identified challenges as well as formalising the value of consent itself, and we hope that the challenges and opportunities identified here may also encourage other researchers to begin tackling the challenges, and realising the value, of consent.

ACKNOWLEDGEMENT

This research was supported by Research Councils UK via the Meaningful Consent in the Digital Economy Project, grant reference EP/K039989/1.

REFERENCES

Anon, 2009.DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, European Union.

ARTICLE 29 DATA PROTECTION WORKING PARTY, 2015. Press Release. Available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20150217__wp29_press_release_on_cookie_sweep_.pdf

Böhme, R. & Köpsell, S., 2010. Trained to accept? *In Proceedings of the 28th international conference on Human factors in computing systems* - CHI '10. New York, New York, USA: ACM Press, p. 2403.

Cradock, E., Millard, D. & Stalla-Bourdillon, S., 2015. Investigating Similarity Between Privacy Policies of Social Networking Sites as a Precursor For Standardization. *In Proceedings of the 24th International Conference on World Wide Web Companion*.Florence, Italy pp. 283–289.

Ermakova, T. et al., 2014. Privacy Policies and Users' Trust: Does Readability Matter? *Twentieth Americas Conference on Information Systems*, Savannah, Georgia, USA, pp.1–12.

Friedman, B., Howe, D. & Felten, E., 2002. Informed consent in the Mozilla browser: Implementing value-sensitive design. *In Proceedings of 35th Hawaii International Conference on Systems Sciences*.Hawaii, USA, pp. 1–10.

Gomer, R. et al., 2013. Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies through Search. *In 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*. IEEE, Atlanta, GA, USA, pp. 549–556.

Howe, N. & Strauss, W., 2000. Millennials Rising The Next Great Generation, Vintage

Kahneman, D. and Tversky, A. 1984. Choices, Values, and Frames.*American Psychologist*, 39, 341-350.

Kelley, P.G. et al., 2012. A conundrum of permissions: Installing applications on an android smartphone. *In Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).pp. 68–79.

Kelley, P.G. et al., 2009. A “nutrition label” for privacy.*Proceedings of the 5th Symposium on Usable Privacy and Security SOUPS 09*,Moutain View, CA, USA,, p.1.

Liccardi, I. et al., 2014. No technical understanding required: Helping users make informed choices about access to their personal data. *In Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services.*London, UK.

Mayer, J.R. & Mitchell, J.C., 2012. Third-Party Web Tracking : Policy and Technology. *In Proceedings of the 2012 IEEE Symposium on Security and Privacy.*San Francisco, USA, pp. 413–427.

Mcdonald, A.M. et al., 2009. A Comparative Study of Online Privacy Policies and Formats.PETS ’09 *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies,*Seattle, WA, USA 5672, pp.37–55.

Shklovski, I. et al., 2014. Leakiness and Creepiness in App Space : Perceptions of Privacy and Mobile App Use. *In Proceedings of the 32nd annual ACM conference on Human factors in computing systems* - CHI ’14. Toronto, Canada, pp. 2347–2356.

APPENDIX A:

TABLES OF DISCLOSURE STATEMENTS

Table 1. Facebook and Google’s Privacy Policy statements

PS1	We do not share personal information with companies, organizations and individuals outside of Google unless we have your consent.
PS2	We may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes: Device information; Log information; Location information; Unique application number; Local storage; Cookies and anonymous identifiers.
PS3	We use technologies like cookies, pixels, and local storage (like on your browser or device, which is similar to a cookie but holds more information) to provide and understand a range of products and services.
PS4	Cookies are small pieces of data that are stored on your computer, mobile phone or other device. Pixels are small blocks of code on webpages that do things like allow another server to measure viewing of a webpage and often are used in connection with cookies.
PS5	For many ads we serve, advertisers may choose their audience by location, demographics, likes, keywords, and any other information we receive or infer about users.
PS6	We process personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.
PS7	You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, its important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.
PS8	We use Cookies, pixels and other similar technologies to: [Make our service easier or faster to use]
PS9	We use Cookies, pixels and other similar technologies to: [Protect you, others and ourselves]
PS10	Many of our services require you to sign up for an account. When you do, we ask for

	personal information, like your name, email address, telephone number or credit card.
PS11	We and our partners use various technologies to collect and store information when you visit a Google service, and this may include sending one or more cookies or anonymous identifiers to your device.
PS12	People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used.
PS13	Your trust is important to us which is why we don't share information we receive about you with others unless we have: received your permission; given you notice, such as by telling you about it in this policy; or removed your name and any other personally identifying information from it.
PS14	We share information we have about you within the family of companies that are part of Facebook.

Table 2. App permission requests

PER1	Your personal information: Read contact data, write contact data
PER2	Services that cost you money: Directly call phone numbers send SMS messages
PER3	Your messages: edit SMS or MMS, read SMS or MMS, receive MMS, receive SMS
PER4	Your location: fine (GPS) location
PER5	Network communication: full Internet access
PER6	Storage: modify/delete SD card contents
PER7	Phone calls: read phone state and identity
PER8	Hardware controls: take pictures and videos
PER9	Read your calendar
PER10	Read your browser's history and bookmarks

Table 3. App permissions requests – willingness to pay in app scenario

App P1	Access coarse location sources such as the cellular network database to determine your approximate location.
App P2	Access fine location sources such as the GPS.
App P3	Access extra location commands to interfere with the operation of the GPS or other location sources.
App P4	Access your precise location using GPS or network location sources such as cell towers and Wi-Fi.
App P5	Receive and process your new SMS texts.
App P6	Read all your SMS texts stored on the phone.
App P7	Read your phone number and serial number.
App P8	Read all your contact (address) data.
App P9	Read a list of all your accounts.
App P10	Read all your calendar events including those of friends and coworkers.
App P11	Read all URLs you visited and all the browser bookmarks.
App P12	Take pictures and video with the camera at any time.

Table 4. Cookie notices (text equivalent)

CN1	GOV.UK uses cookies to make the site simpler. Find out more about cookies.
CN2	We would like to place cookies on your computer to help us make this website better. By continuing to browse this site you are consenting to this.
CN3	By accessing, continuing to use, or navigating throughout this site you accept that we will utilise certain browser cookies to improve the experience, which you receive with us. William Hill do not use any cookies which interfere with your privacy, but only ones which will improve your experience whilst using our site, please refer to our FAQs for further information on our use of cookies and how you prevent their use should you wish.
CN4	ASOS uses cookies to ensure that we give you the best experience on our website. If you continue we assume that you consent to receive all cookies on all ASOS websites.
CN5	We use cookies to ensure we give you the best experience on our website. If you continue, we'll assume that you are happy to receive all cookies on the Transport for London website.
CN6	Santander uses cookies to deliver superior functionality and to enhance your experience of our websites. Read about how we use cookies and how you can control theme here. Continued use of this site indicates that you accept this policy.
CN7	By using this site you agree to the use of cookies for analytics, personalised content and ads.