EXPLORING USER PERCEPTIONS OF ONLINE PRIVACY DISCLOSURES

Helia Marreiros[a] h.marreiros@soton.ac.uk
Richard Gomer[b] r.gomer@soton.ac.uk
Michael Vlassopoulos[a] m.vlassopoulos@soton.ac.uk
Mirco Tonin[a] m.tonin@soton.ac.uk
m.c. schraefel[b] mc@ecs.soton.ac.uk

University of Southampton
Economics Division. School of Social Sciences
SO171BJ Southampton, UK

University of Southampton
Electronics and Computer Sciences
SO171BJ Southampton, UK

ABSTRACT

As a result of various industry regulations service providers such as websites and app developers are required to explain the ways in which they process the personal data of service users. These "privacy disclosures", which aim to inform users and empower them to control their privacy, take several forms. Among these forms are the privacy policy, the cookie notice and, on smart phones, the app permission request. 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. User understanding of the actual content of these disclosures, and their feelings toward it, are less well understood, though. In this paper we report on a mixed-methods study that explored these three types of privacy disclosure and compare their relative merits as a starting point for the development more meaningful consent interactions. We identify four key findings – heterogeneity of user perceptions and attitudes to privacy disclosures, 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, and the possibility that consent interactions are valuable in themselves as a means 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 helps 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 the second about cookie notices, there is significant heterogeneity in users' perceptions and feelings towards statements taken from privacy policies, and cookie notices. In the first survey we show that users consider that some privacy policies reflect a positive attitude of the service provider towards their users, others a negative attitude and others are more neutral.

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, eg (Kelley 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. 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 means 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 (Friedman et al. 2002) describe six components of informed consent as: 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). Disclosure, comprehension and competence are highly dependent on the content that is provided to the user, while voluntariness, agreement and minimal distractionthe last three components 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. Numerous behavioral biases and cognitive shortcuts such as habituation (Böhme & Köpsell 2010) make meaningful and informed consent problematic for human beings and so while the content of the 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, 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 privacy policies of online services providers as Facebook and Google are highlighted and what their understanding is of those privacy policies.

2.4 App Permissions

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.

The use apps on smart phones, such as the iPhone or Android platforms, 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).

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

We conducted an exploratory study that combines two consecutive studies about online behavior and online privacy concerns of the "millennial generation." The first is a focus group study and the second is an online survey.

3.1 Focus group study

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 (our university, redacted for blind review) by means of mailing lists and personal invitation, although some participants were drawn from other departments. We provided participants with pizza during the session. 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 study

The second part of the study took the form of an online survey. 99 "millennial" participants were recruited primarily from (our university, redacted for blind review) 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 2 in appendix A). The 14 privacy policy statements were selected from a larger selection of 25, based on ratings provided by participants in 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).

We conducted a second survey in which 33 participants were shown seven cookie notices and asked to rank whether they felt each one was positive, negative or neutral (See table 3 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

We report the results of the focus study and the online survey study, concerning cookies and online tracking, privacy policies and app permission requests. We focus on participants' understanding and concerns related to each type of disclosure.

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.

4.1.1 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, for instance by remembering previously visited pages to personalize navigation. 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.

Participants were confused about the difference between cookies and browser features such as auto-complete and browser history. A number of participants spoke about the "private browsing" feature of modern web browsers, as a way to avoid being tracked if they wanted to do so, although it was unclear to what extent they made use of this feature themselves.

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.

Only a few participant linked cookie use with behavioral profiling, and only a few of the participants suggested that an advertising network like DoubleClick might have data that had been collected about their browsing history using persistent third party cookies. Participants did not realise that Facebook also has access to partial browsing history through their "share" and "like" widgets.

4.1.2 Privacy Statements

Participants were mixed in their responses to the individual privacy statements. Statements that referred to "protecting" privacy or of 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 that "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.

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.

4.1.3 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 then 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. One participant discussed how different combinations of permissions might pose different privacy risks, for instance by combining access to contact data with the ability to transmit that information outside of the phone via the network access permission.

4.1.4 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.

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 that refer that they don't care about their privacy or how the online services providers are using theirs and others personal data; the "Scary," 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. And finally it helped us to choose the privacy policy statements, app permission requests and cookie notices to be used in the online surveys.

4.2 Online survey study

The second part of the study comprises two online surveys. In the first survey 66 participants were asked to answer questions about statements taken from the privacy policies of Google and Facebook and some permissions taken from Android. In the second survey 33 participants were asked questions about cookie notices. We present each of the three types of privacy disclosure here.

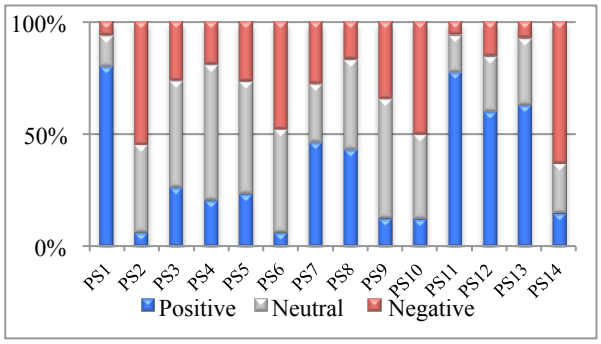
4.2.1 Privacy Policies

Figure 1 shows the percentage of participants that ranked each of the privacy policy statements as positive, neutral or negative. 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 positive. On the other hand statements that suggest data is going to be collected and shared, for example PS2, PS10 and PS14, are considered negative. Statements about cookies – such as their definition and usage - are normally considered 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, considering as positive those that refer to protect their data and personalization and negative those that indicate data collection and sharing.

Figure 1: Privacy policy ratings



4.2.2 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.

Figure 2: Apps permissions' rating 7 likert-scale

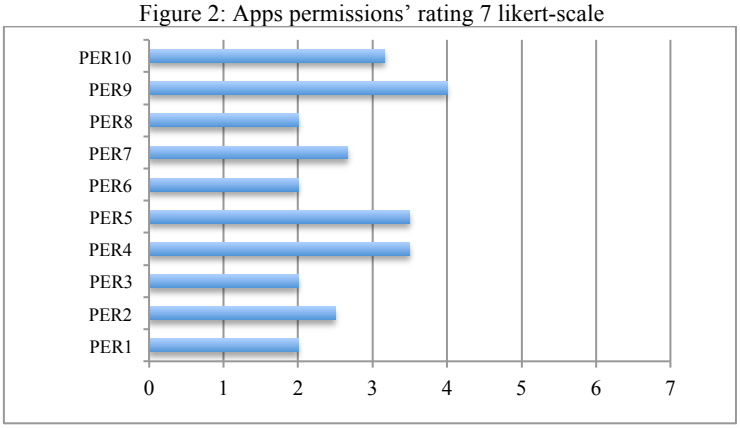
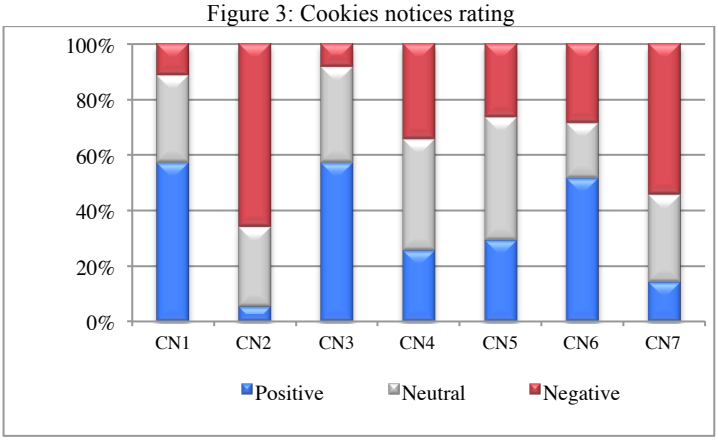


Figure 3: Cookies notices rating



4.2.3 Cookies

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. Nevertheless, as seen in figure 3 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. 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 own 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. The one notable exception to this are the permissions to make phone calls or send SMS messages – Users are notified that these permissions may cost them money. 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 judgements 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 the 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 – although preliminary and based around deliberately open-ended and exploratory methods - 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. Future work should address the identified challenges and formalise the value of consent itself.

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 [Accessed February 15, 2015].

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. Available at: http://dl.acm.org/citation.cfm?id=1753326.1753689 [Accessed July 5, 2012].

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*. pp. 283–289.

Ermakova, T. et al., 2014. Privacy Policies and Users' Trust: Does Readability Matter? *Twentieth Americas Conference on Information Systems*, (Pollach 2007), pp.1–12.

Friedman, B., Howe, D. & Felten, E., 2002. Informed consent in the Mozilla browser: Implementing value-sensitive design. In *Proc 35th Hawaii Intl Conference on Systems Sciences*. pp. 1–10. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=994366 [Accessed January 17, 2014].

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, pp. 549–556. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6690064 [Accessed May 22, 2014].

Howe, N. & Strauss, W., 2000. *Millennials Rising The Next Great Generation*, Available at: http://www.amazon.com/dp/0375707190.

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*, 1990, p.1. Available at: http://portal.acm.org/citation.cfm?doid=1572532.1572538.

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*. Available at: http://eudl.eu/doi/10.4108/icst.mobiquitous.2014.258066.

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*. 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*, 5672, pp.37–55. Available at: http://dl.acm.org/citation.cfm?id=1614507.1614511.

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*. pp. 2347–2356.

Appendix A: Tables OF DISCLOSURE STATEMENTS

Table 1: Facebook and Google's Policy Privacy 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: 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.