

Industry Ideals and Barriers in Using Alternative Privacy Policies

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

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

While privacy policies were developed with the aim of helping users understand their participation in the data economy, they often fail to serve this purpose. Highly complex and extensively lengthy policies have resulted in extremely low levels of user interest and engagement, leading to the users being unaware of the personal data exchange they are involved in. There is an increasing interest in industry to shift from this pattern and move towards alternative models of privacy policies that are more engaging and less intimidating to the average user. In this paper, we outline the results of an industry workshop that explores service provider views, ideals and challenges associated with the move towards alternative models of privacy policies. The results show that providing accountability and maintaining a sustainable and trustworthy customer relationship are the key drivers for this move and focusing on user-centered data practices that enables more active user participation in this scenario is the prescribed method for this shift. The call for interdisciplinary involvement to help cater to the technological, legal, regulatory and ethical demands of this move are also highlighted.

Privacy. Privacy policy. Workshop. Industry. Barriers. Ideals. Attitudes.

1. INTRODUCTION

Current data privacy principles and privacy laws turn upon the individual's active participation in the data economy. This can be traced back to Westin's conception 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' (Westin 1968:7).

Privacy notice and choice has been identified as a potential method (Cranor 2012) in enabling users to understand their role in the personal data ecosystem. A privacy policy is a document that aims to notify a user of the data practices of a service. They share information about the collection, use, sharing and retention of a user's data. Effectively, privacy policies should enable the user to make informed decisions regarding the use of their data. But often, they are ineffective by design (Brandimarte & Acquisti 2013; Ackerman & Mainwaring 2005).

The traditional notice and choice model has resulted in privacy policies that are rarely read or understood by consumers (McDonald & Cranor 2008). Policies have often become a vestigial idea of what once would have been a grand plan to help users comprehend their capabilities and limitations in a data exchange scenario. Currently they mostly

exist to satisfy regulatory bodies as opposed to serving their true purpose of helping the users.

What most industry stakeholders are realising is that empowering the user with knowledge about the data they share would result in enhanced user participation (Rose et al. 2012). Increased user involvement in the digital economy would not only result in better quality and quantity of data but it could also lead to enhanced trust and greater longevity of relationship with the service provider. All of this culminates in a sustainable cycle of data sharing and improvement in quality of services, leading to substantially greater profits (Dean et al. 2012). Owing to these benefits, recently there has been a shift towards alternative privacy policy models, both in academia (Kelley et al. 2009) and industry (Zynga 2011), that are less text intensive and designed to increase user engagement. But these alternatives are yet to be adopted on a global scale.

We, a UK based media organisation, are trying to develop alternative models of privacy policies for our services, that would result in higher user engagement and data legibility. To support this initiative, we ran a workshop as part of our formative studies to help understand service provider wants and needs associated with an ideal privacy policy and the barriers they feel should be overcome to achieve it

2. BACKGROUND

Recently, there has been increased interest in privacy policies on a multi-disciplinary and international level. Regulatory bodies are calling for more engaging versions of privacy policies, industry stakeholders are trying to match regulatory expectations while also balancing their company's best interests and academics from diverse disciplines are congregating to help step away from traditional text rich privacy policies to more interactive and interesting alternatives.

2.1 Need for regulatory compliance

Providing notices is an essential aspect of privacy and data protection legislation, and it requires legal and regulatory compliance. European Data Protection directives (European Parliament & European Commission 1995) have made it mandatory to provide users with privacy policies to ensure ethical exchange of data. In the U.S., the Federal Trade Commission has been regulating the same since the Fair Credit Reporting Act of the 1970s (Federal Trade Commission n.d.). Policies are often expected to serve multiple and contradictory roles (Schaub et al. 2015). Whilst policies may be meeting legal requirements, they are not successful in fulfilling obligations to end-users (McDonald & Cranor 2008; Cranor 2012; Schaub et al. 2015) as the lengthy legal jargon is often inaccessible to the non-specialist.

2.2 Need for Accountability and Trust

While the companies are accountable to regulatory bodies, the present system of accountability is flawed. Once there is a breach of security or privacy, the process consists of pleading for forgiveness from the customers and making settlements with regulators (World Economic Forum & Boston Consulting Group 2012). There has to be a shift in this scheme from that of inefficient cure to effective prevention. For this, accountability has to be built into the business models and technological frameworks of organisations. The principle of accountability is discussed in the draft EU and US legislation (House 2012; EU GDPR n.d.; European Commission 2012). Privacy policies provide a starting point for this principle to be applied. It informs the user of the accountability and enforcement mechanisms offered to them by the companies and governments.

A Europe-wide study conducted in 2010, showed that 70% of consumers were concerned about how companies were using their personal information ((Ec) 2011). This shows an evident lack of trust from the users' side. Building accountability into the data economy through measures like comprehensible privacy policies would help build trust into this scenario. Trust helps not only with

improved brand identity and longevity of customer relationships but it also feeds directly into the efficiency of data-driven services. It is reported that consumers who are able to manage and protect their privacy are up to 52% more willing to share information than those who are not (Rose et al. 2012). Improving trust through user empowerment builds a sustainable cycle of better and more accurate data and thus improved services. Therefore, the best interests of companies, users and researchers are no longer orthogonal and so there is a need to strive towards privacy policies that are more legible, useable and useful to the users so that all parties benefit to the fullest.

2.3 Need for contextual integrity

Researchers have been advocating solutions that help improve the current format of privacy policies. Previous studies on the use of icons (McDonald & Cranor 2008), timing (Good et al. 2007) and appropriate level of settings have informed discussions around the design and development of privacy notices. Alternative layouts like the multi-layered approach (Pinnick n.d.), nutrition label approach (Kelley et al. 2009), P3P policy presentation tool based on the Expandable Grid (Reeder et al. 2008), Audience View (Lipford et al. 2010), Privacy Bird (Cranor et al. 2006) etc have been proposed before. Even with this wide and emerging set of solutions at hand, there is still a call for further research (Schaub et al. 2015) in this area as the majority of the most accessed privacy policies still follow the traditional, text-intensive format.

While the most appropriate of these solutions could be applied to yield better user engagement, it is worth taking into consideration that contextual integrity (Nissenbaum 2004) is a highly debated contributing factor when building privacy enhancing technologies. Users prioritise data differently when interacting with different sectors (Rose et al. 2012) of the industry and hence their trust in the data transaction varies correspondingly (World Economic Forum & Boston Consulting Group 2012). Therefore, with the aim of producing the most effective privacy policy for a user interacting with a media service, we began our research with a workshop that elicited information from company stakeholders on what were the organisational priorities and barriers in implementing an alternative privacy policy.

We believe that the results of this workshop, along with support from the exemplary work from previous research in usable privacy will lead us to a more effective privacy policy that helps the user make informed decisions about one's involvement with data driven and IoT enabled media services and helps organisations by building a sustainable data exchange system that is embedded in trust and user satisfaction.

3. WORKSHOP DESIGN

The aim of our workshop was to outline service provider views of privacy policies, their notion of best practices and the challenges they face in the practical implementation of these goals. The eight participants of the workshop worked in a variety of teams, acting in diverse roles including researchers, computer scientists, software architects, psychologists, project leads etc.

The workshop started with a short welcome by the facilitator, which introduced the participants to the aims and essence of the workshop. The introduction was followed by a quick brainstorming session where the participants filled a white board with terms that they associated to privacy. This was followed by a more focused discussion about privacy policies. Due to the contrast between the diverse nature of the participants' backgrounds and the focused nature of the intended discussions, the facilitator used a general overarching text based privacy policy used by our organisation as a probe (Gaver 2001; Hemmings et al. 2002) and used the principles of Human Data Interaction (Mortier et al. 2013) (legibility, negotiability and agency) as a framework to guide the discussions.

During the course of the workshop, the three principles were revealed to the group and they were asked to discuss their understanding of the principle and the best practices that could make the principle practical for their privacy policy. Following this, the group brainstormed barriers and constraints that prevented them from applying these principles to their privacy policy.

4. FINDINGS

The findings of the workshop could be categorised into the three principles used to guide the workshop discussions. All findings do not strictly belong to just one principle, they have been added to the principle that resonates most profoundly with them.

4.1 Legibility

Legibility encompasses transparency and comprehensibility. Participants were particular about the proper application of these principles as they believed that it was closely related to many of the ideals upheld by our organisation, including maintaining a sustainable and trust worthy relationship with the users. One of the biggest barriers stated by the participants here were regulatory restrictions. They often thought that moving to alternative models could lead to omission or biasing of important information, which could make them more vulnerable towards regulatory reprimands. An array of wants and needs were stated to improve legibility of policies. These include the use of iconography, use of consistent models and terminology, use of simple

language, provision for prioritising information through personalisation, use of summaries, inclusion of data visualisations, availability of different languages, improved accessibility etc.

4.2 Negotiability

Negotiability triggered a discussion on affording the user with choices by going beyond the currently available binary yes or no consent forms. Giving the user more avenues for involvement was considered to result in an enhanced user relationship with the company and increased trust in the organisation. Different methods for providing granular consent were discussed, including notifications, alerts, updates, emails etc but the balance between probing and spamming was left unresolved. Key barriers here were related to understanding the optimum amount of choices presented to the user so that fatigue, disinterest and intimidation were minimised.

4.3 Agency

Discussions about agency leaned on control. Questions about the user's right to control one's data, the concept of data being relational (Crabtree & Mortier n.d.) and not just about one person and hence the division of control etc were touched upon. Relating to privacy policies, the need for actionable control, which was often related to negotiability, was deemed necessary. But demanding the user to make privacy choices through data control before experiencing the technology and learning the associated benefits and implications was considered a weakness in the current models.

5. RECOMMENDATIONS

The findings of the workshop reflect on the current need for industry to actively adopt measures to help make privacy policies more useful and useable. The interdisciplinary nature of the HCI community makes it the perfect avenue for such solutions that involve the blend of design, policy and technology, to be feasible. We put forward a discussion that outlines the aspects of this scenario that we believe requires immediate attention.

5.1 Accountability

The discussions often focused on the need for maintaining the trust users have in the organisation. This reflects the need for accountability provided by the organisation. Accountability in the scenario of personal data collection and use is identified in The Consumer Privacy Bill of Rights (Federal Trade Commission n.d.) in the US and the GDPR (EU GDPR n.d.) in the EU.

For accountability to be fully realised, the user should know and understand the privacy policy. Providing increased legibility through iconography and sample data visualisations in the privacy policy would help the users understand the complete meaning of the agreement they are entering. Thus, the privacy policy could be utilised as a space for service providers to effectively present the organisation's efforts to ensure accountability.

5.2 Support for sustainability of relationships

One of the barriers in designing more effective privacy policies is the hypocrisy presented by the juxtaposition of the need for an on-going customer relationship and the demand for approval of the privacy policy even before that relationship begins.

For privacy policies to be useful to the user, it has to be served in a manner that is meaningful to the user as opposed to exploiting the moment when the user is most keen on experiencing the service and hence places more value on the service rather than the data shared (Acquisti & Grossklags 2004). There has to be ways of temporally contextualising the need for collected data. This could be through updates and alerts that let the user know of spikes in data collection and options for changing permissions. Providing the user with dashboards, user profiles generated by the organisation through data collection or even monthly statements of data use are all additions that could support a privacy policy in its move towards enabling sustainable customer relationships. HCI researchers could contribute significantly in this domain by looking into more alternatives that deliver the privacy policy in forms and times that are meaningful to the user.

5.3 User centred data practices

One of the over arching themes drawn from the discussion was the importance of making the users understand the value of their contribution and the need for their active participation in the data economy.

While reading the privacy policy marks the beginning of one's involvement with a service and it's associated data trail, it is also a medium for helping the users understand their role in this complicated scenario. Mechanisms for improved legibility, like a shift from text rich formats to iconography or other alternative formats and personalisation of privacy policies are potential avenues worth further exploration. Solutions that give the user more avenues for actionable control while involving with a privacy policy are desirable. This is worth exploring also because research has shown that users associate very low value to reading privacy policies as the only options available are to accept or decline them as a whole (Cranor 2012).

HCI research could help solve many problems in this space by looking into alternative models that go beyond just iconography and summaries to options that enable better user engagement like policy personalisation. Another avenue that demands more attention is exploring and evaluating the optimised mix of controls that would encourage the user to get more involved with privacy policies while not feeling overwhelmed, intimidated or fatigued.

5.4 Need for interdisciplinary intervention

The shift towards more effective privacy policy models is slowed down by a number of challenges that include legal restrictions, regulatory barriers, company policy, technological limits, etc. To overcome these barriers, there is the need for an interdisciplinary intervention with the involvement of experts from legal, technical, user experience and design working together to strive towards solutions that encourage better user engagement with privacy policies. HCI's multi-disciplinary positioning gives its researchers the unique right to play a key role in this scenario by helping promote research and involve in discussions that delve into the creation and successful deployment of useable privacy policies.

6. CONCLUSION

The many benefits attached to increasing user trust is pushing industry stakeholders to invest more in privacy enhancing measures. As part of this initiative, there is an interest in moving away from current text-rich privacy policies to more engaging and effective models. But for this herculean shift to be practical, there should be an understanding of the key drivers and barriers that are affecting this move.

This paper presents the results of an industry-led workshop involving service providers working in diverse capacities expressing their notions associated with designing alternative privacy policies. The discussions show that the need for accountability and the purpose of having sustainable and long-term customer relationships are the key drivers for this shift. Service providers identify focusing on user-centered data practices that encourage more active user participation in the data economy to be an effective method for increased engagement and interest in privacy policies. The discussions also highlight the need for an interdisciplinary intervention that brings together technology, design, research, law, regulations and ethics, for the proposed shift to be practical.

Having mapped the industry views and ideals associated with this scenario, we believe that HCI research, with its interdisciplinary capacity is in a unique position to map these priorities to effective design solutions, thus bringing this effort to realisation.

7. REFERENCES

- (Ec), E.C., 2011. SPECIAL EUROBAROMETER 359 Attitudes on Data Protection and Electronic Identity in the European Union. , p.330. Available at: http://ec.europa.eu/public_opinion/index_en.htm.
- Acquisti, A. & Grossklags, J., 2004. Privacy attitudes and privacy behavior. *Economics of Information Security*, pp.165–178.
- Crabtree, A. & Mortier, R., Human Data Interaction : Historical Lessons from Social Studies and CSCW. *ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway*, pp.3–21.
- Cranor, L., 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* Available at: http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jtelhtl10§ion=22 [Accessed September 16, 2016].
- Cranor, L., Guduru, P. & Arjula, M., 2006. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 13(2), pp.135–178.
- EU GDPR, Home Page of EU GDPR. Available at: <http://www.eugdpr.org/>.
- European Commission, 2012. Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *COM (2012) 11 final, 2012/0011 (COD), Brussels*, 11, p.118.
- European Parliament & European Commission, 1995. Directive 1995/46/EC on protection of individuals with regard to the processing of personal data on the free movement of such data. *Official Journal of the European Communities*, (L281/31), pp.31–39.
- Federal Trade Commission, Protecting Consumer Privacy | Federal Trade Commission. Available at: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy> [Accessed January 11, 2017].
- Gaver, W., 2001. Cultural Probes- Probing People for Design Inspiration. *SIGCHI. DK*.
- Good, N.S. et al., 2007. Noticing notice: a large-scale experiment on the timing of software license agreements. *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '07*, p.607.
- Hemmings, T. et al., 2002. Probing the Probes. *PDC*, (June), pp.42–50.
- House, W., 2012. Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. *White House, Washington, DC*, pp.1–62.
- 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>.
- Lipford, H.R. et al., 2010. Visual vs. compact. *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, p.1111. Available at: <http://dl.acm.org/citation.cfm?id=1753326.1753492>.
- McDonald, A.M. & Cranor, L.F., 2008. The Cost of Reading Privacy Policies. *I/S - A Journal of Law and Policy for the Information Society*, 4(3), pp.1–22.
- Mortier, R. et al., 2013. Human-Data Interaction : The Human Face of the Data-Driven Society.
- Nissenbaum, H., 2004. Privacy as contextual integrity. *Wash. L. Rev.*, pp.101–139. Available at: http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/washlr79§ion=16.
- Pinnick, T., Layered Policy Design | TRUSTe. Available at: <http://www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/> [Accessed January 11, 2017].
- Reeder, R.W. et al., 2008. A user study of the expandable grid applied to P3P privacy policy visualization. *Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain V(Xml)*, pp.45–54. Available at: <http://portal.acm.org/citation.cfm?id=1456413>.
- Rose, J., Rehse, O. & Röber, B., 2012. The Value of our Digital Identity. *Liberty Global Policy Series*. Available at: <http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>.
- Schaub, F. et al., 2015. A Design Space for Effective Privacy Notices. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp.1–17.
- World Economic Forum & Boston Consulting Group, 2012. Rethinking Personal Data :

Strengthening Trust. , (May), pp.1–35.

Zynga, 2011. PrivacyVille. Available at:
<https://www.zynga.com/privacy/privacyville>.