Computers in Human Behavior 58 (2016) 368–379

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

When changing the look of privacy policies affects user trust: An experimental study

Esma Aïmeur [a, *], Oluwa Lawani [a], Kimiz Dalkir [b]

[a] Department of Computer Science and Operations Research, University of Montreal, Montreal, Canada
[b] School of Information Studies, McGill University, Montreal, Canada

ARTICLE INFO

Article history:
Received 20 July 2015
Received in revised form
5 November 2015
Accepted 11 November 2015
Available online xxx

Keywords:
Privacy policies
Trust
Format
Economics of privacy
Private data control
Data management

ABSTRACT

The majority of Internet users do not read privacy policies because of their lengthy verbose format, although they are still the main source of information for users about how their data are collected and used. Consequently, as shown by many studies, users do not trust online services with respect to the use of their private data. Furthermore, they find it unfair that their data are used to generate revenue by online services without their knowledge or without their benefit from this.

In this paper, we take as main assumption that the control of their private data and also caring about their interests would restore the trust of users. Based on an empirical model, we conducted an experimental comparative study of user trust by offering to two groups of participants the possibility to adhere to a service with a privacy policy presented in one of two different formats: the first, a conventional privacy policy and the second, designed according to the privacy policy model studied in this paper.

We collected, through a survey, 717 responses from participants. The results show that allowing personalization and management in privacy policies affects user trust and makes online services appear more trustworthy to their users.

1. Introduction

The Internet is used by almost three billion people around the world. Among them, around two billion have a social network account, and 890 million connect to Facebook every day. More than 200 million of those Internet users[1] shopped online in the USA in 2015. Yet many of them do not have trust in these services due to the use of their personal data by the same services. Indeed, in terms of protecting their private data, only 10% of users trust social networks, 20% trust e-commerce sites and 22% trust technology companies in general.[2] In addition, users are increasingly aware of the value of their data, and find it unfair that companies generate revenue from their personal data.

Privacy policies are the channel through which Internet services disclose to their users the data they collect from them and the use that is made of it. Despite the concerns of users regarding their private data, few of them take the time to read the policies before making a purchase or using a service. This is due to the length of the privacy policies and the difficulty of reading and understanding them (Ermakova, Baumann, Fabian, & Krasnova, 2014; Furnell & Phippen, 2012). Knowing that privacy policies are the main source of information for users about the services' privacy practices and the place where users give their consent to those practices, they should be presented in a friendly format allowing users to read and really understand their contents. Add to this the fact that users are practically forced to fully accept the terms of the policy in order to use the service. Users are therefore facing a dilemma where they generally lose as they must select between two unappealing choices. Indeed, either they accept the terms of the policy at the risk of losing their privacy, or they refuse to adhere to the policy and then they do not have access to the service.

In order to ensure the continuity and development of trade on the Internet, Online Services (OSs)[3] must regain the trust of users (Ermakova et al., 2014). In this paper, we hypothesise that users' control over their data, as well as caring about their interests in

* Corresponding author.
E-mail addresses: aimeur@iro.umontreal.ca (E. Aïmeur), lawanio@iro.umontreal.ca (O. Lawani), kimiz.dalkir@mcgill.ca (K. Dalkir).

[1] http://www.statista.com.

[2] State of Privacy Report, Symantec, 2015.

[3] OS: Online Service.

http://dx.doi.org/10.1016/j.chb.2015.11.014
0747-5632/© 2016 Elsevier Ltd. All rights reserved.

exchange for the use of their data can actually help reach this level of trust. As such, we propose a new model of privacy policies. This model is presented in a friendly format and offers users the possibility to manage the data they want to exchange with the OS. In addition, users can receive various rewards depending on the data they disclose to the services.

We conducted a survey where we submit to participants the content of the same privacy policy but in two different formats. Analysing results allows us to contrast users' trust level in an internet service when adhering to it using a conventional privacy policy in comparison to our privacy policy model.

This paper is organized as follows. In Section 2, we explore the state of the art through a literature review, then we present our research and privacy policy model in Sections 3 and 4. Section 5 details our testing methodology, and Sections 6 and 7 highlight and analyses the results. Section 8 concludes this work and presents future works.

2. Related work

2.1. Privacy policies

Privacy policies are the way in which websites inform their users on how they collect and use their data. However, many studies show that these policies are often ignored by users.

More than 50% of Canadians never read privacy policies (Canada, 2013). Only 4% of Internet users regularly read privacy policies while 55% of respondents had never read the terms of the agreement (dos Santos Brito, Cardoso Garcia, Araujo Durao, & Romero de Lemos Meira, 2013). This is due to several factors, such as the length of the privacy policies (Ermakova et al., 2014; McDonald & Cranor, 2008), their non-specific and vague content, and their non-standard formats (Schaub, Breaux, & Sadeh, 2014).

A recent study analysed the current attitudes of individuals towards privacy policies and changes in those attitudes in the last decade by comparing data collected from an online survey in 2014 to a research published by Annenberg Public Policy Center in 2005. Results show that people's attitudes have not changed throughout these years. According to respondents, privacy policies are still too long, too complex and serve mostly to protect organizations (Williams, Agarwal, & Wigand, 2015).

Although privacy policies are still the key source of information for users to know how companies collect, use and share their data, do people really understand the content of privacy policies? A study (Reidenberg et al., 2014) investigate the difference of interpretation among experts and typical users. Their purpose was to analyse if people understand privacy policies enough to make decisions about their confidentiality. To do this, they presented a set of privacy policies to expert and non-expert users and asked them few questions about them. The results show that there were important discrepancies in the interpretation of privacy policies language, mostly with respect to data sharing. This indicates that privacy policies are sometimes unfair and may mislead people's decision making. It also appears that the lack of understanding content of privacy policies is increased by systems and applications including an integration with social networks (Caramujo & da Silva, 2015). In the same spirit, even for those (few) people who take the time to read privacy policies, they often lack the expertise to adequately assess the consequences of agreeing to the collection, usage or disclosure of their personal data (Aïmeur & Lafond, 2013).

Even reading privacy policies has a cost to the user as it takes approximately 76 working days to read all the privacy policies of all websites visited in one year. As a result, users do not really know what information is collected about them and shared with third parties (Richards & King, 2014).

Investigating trust and privacy concerns through the relationships among the content of privacy statements and consumer trust, they found that this relationship was significant (Wu, Huang, Yen, & Popova, 2012). Also, the relationship between consumer trust and willingness to provide personal information was important. It is then important to solve the problems of privacy policies design in order to preserve personal information sharing on Internet.

In the same spirit, one study suggests that OSs should maximize the benefits of the privacy policies' characteristics in order to induce their reading by users. Indeed, the study tested three design elements (length, visibility, and specificity) effectiveness to address information sensitivity, measuring perceived importance and relevance of the policy on the decisions to share personal information. The results showed that visibility and specificity were significant. Visibility had the strongest influence on relevance (Capistrano & Chen, 2015).

Many solutions have been proposed to tackle those privacy policies problems. Recommended by W3C, P3P (Platform for Privacy Preferences) is a project which enables websites to express their privacy policies in a standard format. On the other hand, it also allows users, through software agents, to specify their privacy preferences and then, automate privacy related decision making according to these preferences (W3C). However, only a few websites and users adopt this platform because of its complexity. Also, users do not have the possibility to negotiate with the service on the terms of the policy.

P2U (Purpose-to-Use) is a framework for privacy-aware user data trading based on the purpose of adaptation. Through this framework, applications can offer and negotiate user data sharing with other applications according to a privacy policy defined by the user. This privacy policy specifies the purpose, type of data, retention period and price for user data (Iyilade & Vassileva, 2013). However, how can the user be sure that his preferences are correctly taken into account by applications? It seems important to have a third party who can decide and negotiate with applications requesting user data.

Based on available technologies (P3P and APPEL- A P3P Preference Exchange Language), a new design of privacy architecture for pervasive environments that supports negotiation was proposed (Qwasmi, El-Khatib, Liscano, & Thorpe, 2013). Negotiation not being part of the last version of P3P, they added a negotiation-group to the P3P policy file structure. Their model aims to allow users to control what information is collected, how it is used and under what circumstances it is shared. Even though their goals are similar to those of our paper, their negotiation does not include the value given by users to their data. Moreover, and in contrast to our proposed model, they do not give users many options on each term of the privacy policy, and users cannot decide how their data will be processed.

Rao et al. (Rao, Schaub, & Sadeh, 2014) found that they “elicited surprises and concerns regarding the data in [user] profiles” as users were not aware of the types of data that made up their behavioural profiles and that companies had fairly easy access to this profile data. To make matters worse, this study also found that a large number of profiles were inaccurate. One source of errors was due to the fact that different companies were combining data and few made any effort to validate profile data. The study concludes with a recommendation that companies should get users' explicit consent before combining data from multiple sources.

Few companies are transparent with respect to their data retention times and also, they failed to offer users the ability to consult the information collected about them (Cranor, Hoke, Leon, & Au, 2014). Self-regulation does not appear to provide for sufficient meaningful privacy policy choices to users. In an attempt to solve these problems, PCAST (President's Council of Advisors on