Computers in Human Behavior 55 (2016) 992–1000

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

"I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment

Nili Steinfeld [a, b, *]

[a] The Hebrew University of Jerusalem, Mount Scopus, Jerusalem, Israel
[b] Ariel University, Ariel, Israel

ARTICLE INFO

Article history:
Received 7 August 2014
Revised 2 June 2015
Accepted 24 September 2015
Available online 18 November 2015

Keywords:
Privacy
Computer-mediated communication
Privacy policies
Eye tracking
Experiment
Decision making

ABSTRACT

Privacy policies are widely used by online service providers to regulate the use of personal data they collect, but users often skip on reading them and are unaware of the way information about them is being treated, and how they can control the ways in which that information is collected, stored or shared. Eye tracking methodology was used to test if a default presentation of a policy encourages reading it, and how the document is being read by users. Results show that when a privacy policy is presented by default, participants tend to read it quite carefully, while when given the option to sign their agreement without reading the policy, most participants skip the policy altogether. Surprisingly, participants who actively choose to read the policy spend significantly less time and effort on reading it than participants in the default condition. Finally, default policy presentation was significantly related to understanding user rights and restrictions on the use of personal data.

1. Introduction

Privacy policies are the common method for online service providers to regulate their engagement with users, but they are also used by users to supervise the way personal data is treated by companies. Still, despite their importance to users, previous research shows that these policies are often ignored (Acquisti & Grossklags, 2005; Angulo, Fischer-Hübner, Pulls, & Wästlund, 2011; Kesan, Hayes, & Bashir, 2012; McDonald & Cranor, 2008; Meinert, Peterson, Criswell, & Crossland, 2006; Nissenbaum, 2011; Tsai, Egelman, Cranor, & Acquisti, 2011). In the current research, eye tracking was used to study reading patterns of a privacy policy and how a default presentation of a policy encourages reading it. The study relies on the theory of status quo bias in decision making, according to which framing a specific behavior as the status quo creates a bias towards this behavior (Korobkin, 1998; Kahneman, Knetsch, & Thaler, 1991; Samuelson & Zeckhauser, 1988). While previous research focused on users' statements regarding reading policies, or on choices made by users in online contexts, this study utilizes eye tracking methodology to actually learn how these policies are being read, empirically test the theory of status quo bias in encouraging reading privacy policies among internet users, and accordingly-on their knowledge regarding authorized and prohibited uses of personal data.

2. Literature review

A website's privacy policy, usually embedded into its general "Terms of Service" agreement, is a document regulating the relationship between the user and the site. These policies are usually drafted by lawyers and are designed to limit companies' legal liability (Earp, Antón, Aiman-Smith, & Stufflebeam, 2005). In many cases, a privacy policy is legally required or normatively expected of service providers. In the US, organizations engaged in electronic commerce are compelled to follow the Fair Information Practices guidelines, a set of widely accepted principles summarized by the Federal Trade Commission regarding the collection, use, and dissemination of personal information (Federal Trade Commission, 2000). Most websites use a terms and conditions document to address these principles (Antón, Earp, & Carter, 2003; Hui, Teo, & Lee, 2007; Milne, 2000). European organizations are bound by the European Union's Data Protection Directive, which is more restrictive than the American law (Antón et al., 2003).

Privacy policies are also the main tool for users and data protection groups to review and supervise a company's conduct. In numerous cases, companies have been accused of and sued on the basis of their privacy policies' violation of state privacy laws

* Ariel University, Ariel, Israel.
E-mail address: nilisteinfeld@gmail.com

http://dx.doi.org/10.1016/j.chb.2015.09.038
0747-5632/

(BBC., 2013a, 2013b; Goel & Wyatt, 2013; Pfanner, 2012; Seshagiri, 2013) or for violating their own (or other services') privacy policies (BBC., 2012; Chellel & Hodges, 2012; Kravets, 2013; Rosenblatt, 2012; Womack, 2013).

Privacy policies contain information that can empower users, by making clear what their rights are and what options they have to better control the use of data about them (for example, if they can opt out of third-party information sharing). The information given in a privacy policy sets the boundaries for the use of personal data by companies, and as described above can provide a basis for lawsuits against companies. In addition, in many cases the policy explains the ways in which users can control how and what information about them is being collected and stored: For example, in Google's privacy policy, the document provides links to services that enable users to see or get a copy of their data (Google, n.d.). In Facebook's privacy policy the document provides links and explanations on how to control privacy settings, download a user's stored information, deactivate or delete an account (Facebook, n.d.). But as previous research shows, most users rarely read these policies. Since agreeing to the terms of the policy is usually a prerequisite for subscribing to a website or a web service, most users sign their agreement to them almost automatically, and these terms are rarely considered as reasons for joining or avoiding a website (Acquisti & Grossklags, 2005; Angulo et al., 2011; Kesan et al., 2012; McDonald & Cranor, 2008; Meinert et al., 2006; Nissenbaum, 2011; Tsai et al., 2011). However, while the policies themselves may not lead users to avoid a service, a number of recent studies by Pew research center found that users, adults and teens, have in fact avoided using mobile applications or have uninstalled online services and applications due to concerns about the use of personal information (Pew, 2012; 2013; 2015). When asked why they do not read privacy policies, users offer various reasons, including complexity, legal language, and length (Angulo et al., 2011; Milne & Culnan, 2004; Nissenbaum, 2011; Tsai et al., 2011). Other reasons for not reading privacy policies include their vague language and use of nebulous terms (Antón et al., 2003), their format and font size (Milne & Culnan, 2004), or users' prior acquaintance with the company or brand (Milne & Culnan, 2004). The fact that many policies include a company's right to change the policy at any time without requiring users' consent makes it almost impossible to keep track of a company's policy (Nissenbaum, 2011).

Moreover, it seems practically impossible to read all policies of websites we interact with: McDonald and Cranor (2008) calculated the average time for an average American adult to read every privacy policy and update she encounters in a year, and found that the national opportunity cost (i.e., the national cost of the time spent on reading policies and comparing between different websites on the basis of their policies, at the expense of manufacturing and labor) is roughly $781 billion per year. The researchers state that if all American Internet users read every privacy policy of every new website they visited, the nation would spend about 54 billion hours each year reading these policies, an average of 40 min a day per citizen.

However, not reading privacy policies can have serious implications. When a user is unaware of the terms of her engagement with a company, she may unknowingly consent to certain uses of personal information she does not approve of. These agreements are binding: According to the American Department of Justice, violating a website's terms of use (either by the user or website) is a violation of the Computer Fraud and Abuse Act, which defines computers-related criminal offenses (Kesan et al., 2012).

Users' knowledge of the use of personal data provides a basis for better control over their relationship with the service, and allows making more informed decisions regarding the exchange of data for service. Several studies show that informed users tend to be less anxious with regard to their online privacy, and that willingness to provide information can change dramatically according to the type and sensitivity of information collected by the service (Earp & Baumer, 2003; Meinert et al., 2006; Milne & Culnan, 2004; Milne, 2000; Phelps, Nowak, & Ferrell, 2000; Tsai et al., 2011), and even more so according to the level of security the site offers to protect the information of its users (Belanger, Hiller, & Smith, 2002). Previous research shows that consumers are even willing to pay a certain premium when purchasing online products from websites that guarantee data security and refrain from collecting irrelevant personal information (Jentzsch, Preibusch, & Harasser, 2012; Tsai et al., 2011). However, when required to choose between two different websites, most consumers will purchase a product from the less expensive site, even when it requires more comprehensive data disclosure (Jentzsch et al., 2012). This may be due to the complexity of calculating the cost of disclosing a specific piece of information with a service, when the user doesn't know how that information is treated, distributed, or cross-referenced with other data from various sources, in a process of profiling the user for a variety of agents and companies (Jentzsch et al., 2012; Solove, 2004).

Several recommendations for clarifying privacy policies to make them easier to understand have been proposed by scholars. These include presenting the policy in a multi-layer format, "privacy birds", [1] privacy agents that sum up the main points in a policy, use of visualizations or privacy labels similar to nutritional labeling (Angulo et al., 2011). While making privacy policies easier to comprehend is important and desirable, simplifying the policies would help users who actually read them understand them better, but the challenge of encouraging users to read the policies remains.

Milne and Culnan (2004) discuss the characteristics of users who are more likely to report reading privacy policies on a regular basis. In their research, older participants were more likely to read policies (a finding that contradicts Earp & Baumer, 2003; who found that users under the age of 35 are more likely to read policies). Education was negatively related to reading policies. Women are more likely than men to read policies, and users who express concerns for privacy, or believe the website would follow its policy are more likely than others to report reading policies.

Does presentation of the policy affect users' likeliness to read the policy, and influence the time and effort devoted to reading it? In decision-making theory, much research has addressed the effect of default options on individuals' decisions. If we perceive individuals as purely rational creatures, the framing of a question or situation should not have an effect on users' decisions if it is not consistent with their preferences (Johnson & Goldstein, 2003). In reality, however, it seems that participants in a variety of cases prefer the default option (Johnson & Goldstein, 2003; Samuelson & Zeckhauser, 1988; Kahneman et al., 1991). In other words-when a choice is presented to individuals in a way that frames one option as a default, and the other options as alternatives-they tend to favor the default option. This behavior is well explained by the theory of status quo bias (Kahneman & Tversky, 1984): When individuals are required to make a decision between no-change (retaining the status quo), and another choice or choices, they are biased in favor of the status quo (Kahneman et al., 1991; Korobkin, 1998; Samuelson & Zeckhauser, 1988). All other choices are weighed relatively to the status quo, where possible loss is valued higher than possible gain (Ariely, 2008; Johnson & Goldstein, 2003; Kahneman & Tversky, 1984). Kahneman et al. (1991) explain how preferring

[1] Privacy birds are browser tools that read privacy policies of websites and inform the user if they match her predefined preferences.