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.

the status quo relates to loss aversion:

> In general, a given difference between two options will have greater impact if it is viewed as a difference between two disadvantages than if it is viewed as a difference between two advantages. The status quo bias is a natural consequence of this asymmetry: the disadvantages of a change loom larger than its advantages (p. 200).

Korobkin (1998) uses the notion of regret avoidance to explain the tendency for no-change: "Individuals experience greater regret when undesirable consequences follow from action than when they follow from inaction" (p. 657), which leads them to favor the current state, perceived as inaction in comparison to actively choosing another option.

Status quo bias and the effect of the defaults have been studied with relation to choosing privacy preferences online. Bellman, Johnson, and Lohse (2001) and Johnson, Bellman, and Lohse (2002) show that changing the default in a privacy preference leads to substantial differences in agreement rates to that preference. Users tend to choose the default privacy preference, when a default exists.

3. Research questions

There seems to be a gap between evidence showing users' wish to be informed of the use of their personal information, and their own statements about not reading privacy policies. How, then, can this gap be explained?

One possible reason for the gap relates to the complexity of reading policies or influencing the way information is collected or treated by the service provider: Users feel that although they would like to protect their privacy online in principle, this is a much too complicated task in practice, and they give up trying to be aware and maintain control, both because they feel it's a hopeless struggle they can't win, and because actually reading all policies they encounter seems an impossible mission.

Another possible reason that has received little academic attention is websites' strategy to request users to accept the terms without presenting the policy to the users. Instead, users can (but are not required to) press a link that leads to the policy they are asked to accept. This study focuses on such a presentation strategy, and examines the effect of privacy policy presentation on users' willingness to read the policy. According to the theory of status quo bias and the default effect, we would assume that users who are required to accept a policy presented to them by default on the screen will be more likely to read the policy than users who are asked to accept the policy's terms without it being presented to them by default. Where the default is no-action, or not reading the policy, the effort in clicking the link to read it may seem too great. Therefore, building on the theory of status quo bias, the hypothesis at the center of this study is:

H1. Users who are asked to agree to a privacy policy presented to them by default will read it more carefully than users who are asked to agree to a policy not presented by default.

Specifically with regard to users who read the policy, the study asks:

(a) How much time do users spend on reading a policy?
(b) Which sections of a privacy policy do users read more carefully?

Furthermore and as previous research shows, we expect users who read the privacy policy to be more informed and educated regarding the use of personal data, and the restrictions imposed on the service provider's use of data it collects. Therefore, the second hypothesis is:

H2. Participants who are presented with the privacy policy by default will have a better understanding of the permitted and prohibited uses of personal data according to the policy, as a result of spending more time on reading the policy than participants who are asked to agree to a policy not presented by default.

The third hypothesis of the current study relates to the characteristics of users who read the policy:

H3. Users who attribute more importance to privacy and privacy policies will read the privacy policy more carefully than users who attribute less important to consider the existence of privacy policies or privacy in general.

4. Method

4.1. Preliminary study

Prior to the current experiment and as a basis for drafting the policy used in the experiment, a preliminary study was conducted to code the privacy policies and registration processes of the 100 most popular websites in the world. The list of popular websites was based on Alexa's top sites for December 21, 2012, [2] which includes leading search engines (Google, Bing), social networks (Facebook, Twitter, LinkedIn, Tumblr, Pinterest, Instagram), news sites (BBC Online, HuffingtonPost, CNN), discussion groups (Stackoverflow), information websites (Wikipedia, About), and others. Of the 100 entries, privacy policies of non-English sites (unless an English version of the privacy policy was available) and local versions of global sites that appeared on the list and share the same privacy policy (e.g., google.uk and google.de) were excluded. Websites with no privacy policy were excluded from the coding as well. In total, 45 privacy policies were coded.

Coding covered policy length, mention of special groups or populations (such as children, members of specific states etc), whether users can inspect the data collected by the service, whether future policy updates require consent from registered users, third-party information disclosure policy, presentation of the policy during the registration process, and other features.

Results show that the average policy length is 2400 words. Only seven (15.6%) of the policies included a paragraph that prohibits the company from modifying the policy without informing registered users, while 18 policies (40%) stated that future changes to the policy made by the company bind all registered users. Slightly over one half (23 policies, or 51.1%) allow the company to share information it collects on its users with third parties for advertising, 18 (40%) allow third-party information disclosure for research purposes, and 35 (77.8%) allow the company to share information with a third party for "improvement of service." Only seven policies (15.6%) informed the users of the option to object to the disclosure of personal information to third parties. Nine (20%) stated that no such option exists, while the remaining 29 policies (64.4%) made no mention of such an option.

In most cases, the privacy policy is part of the general "Terms and Conditions" agreement. No website included in this study presented the policy by default upon registration. In fact, only eight (17.8%) included a link to the policy when presenting the user with a checkbox to indicate her agreement to the "Terms of Service" or privacy policy upon registration. Slightly more than one half (51.1%

[2] Alexa (2012) publishes a list of "top sites" each month, based on the number of logins in the preceding month.

or 23 sites) state upon registration that the user is actively agreeing to the terms of service by pressing the button to create an account. These sites contain no request to mark a checkbox, although a link to the policy is included. The remaining 13 sites (28.9%) state nothing regarding any terms of service upon registration. They do not notify new users on their agreement or present a link to the policy. In such cases, users interested in reading the policy have to search for it on the company's website, which is not always an easy task.

4.2. Study design

After coding the policies, a privacy policy was designed for the experiment. The policy was drafted to match the general style of the policies coded in the preliminary study. It included common policy clauses, terms, and phrases. The policy described the actual restrictions imposed on the researcher regarding the use of data collected on participants during the course of the study. The policy was intentionally more concise than the policies coded in the preliminary study (451 words in Hebrew), so it wouldn't discourage or exhaust study participants.

The study was conducted in a lab at a public university in Israel, using a computer connected to a SensoMotoric Instruments' REDm eye tracker (SMI), a non-invasive device that is based on a panel attached to a computer screen, which measures the participant's eye movements using an infrared eye camera. The device tracks both eyes and requires a very short calibration at the beginning of every session, and operates at a 120 Hz sampling rate (SMI, n.d.), which is sufficient to capture all visual fixations (maintaining gaze on a single location, indicating that the subject is focusing on a visual object).

Each session combined three consecutive eye tracking experiments, and was designed so that the first screen, welcoming the participants, was actually part of the experiment. The welcome screen stated: "Hello and welcome. Before we begin, we ask that you sign your agreement to the Terms and Conditions of the study", and participants were asked to mark a checkbox indicating their acceptance of the "Terms and Conditions". The request resembled (in language and form) the presentation methods used by websites to elicit users' agreement to their policies, as the preliminary study showed. A great emphasis was given to the format of the policy and the text next to the checkbox, so that participants will not identify the request with a common request to sign an informed consent, usually given to participants before the beginning of the experiment. Participants filled a questionnaire prior to entering the lab and for them, the session was already undergoing when they were asked to mark the checkbox. The participants were randomly assigned by a computer program to one of the two study conditions: (a) The default group: The privacy policy is presented to the participants by default, and beneath it the checkbox (unmarked) and the sentence: "I have read and agree to the terms of service"; (b) The non-default group: The checkbox (unmarked) states: "I have read and agree to the terms of service", without a privacy policy presented on the screen. The words "Terms of service" are a link which, if pressed, directs users to a page presenting the exact same policy as in the default group, with the checkbox beneath it-in an identical form as for the default group. The policy discussed authorized and prohibited usage of data collected during the experiment by the researcher. After accepting the Terms, participants continued to a set of activities on the screen, which were related to other eye-tracking experiments. They were not told that the welcome screen was part of the experiment itself. An average session lasted about 5.5 min.

Participants' actions (e.g., whether they pressed the link, how long they stayed on the page featuring the policy) and eye movements were recorded throughout each session. For the analysis of eye movements, each paragraph of the policy was defined as an area of interest (AOI), and the following measurements were analyzed for each AOI: Dwell time (total time spent on the area-fixations and saccades-rapid eye movements between fixations, in ms), Fixation count, Fixation time (in ms), and Entrance time (the time elapsed, in ms, from the loading of the page until the first fixation is measured in the AOI). Entrance time was used to define the order in which users read the policy's paragraphs.

In addition to answering the pre-session questionnaire, after completing the session participants were asked to respond to items concerning their views on privacy and privacy policies, as well as items on the kinds of uses the policy presented at the beginning of the session authorizes or prohibits the researcher with the data collected in the study, to test participants' knowledge of the restrictions imposed on the use of personal data according to the policy.

The sessions took place between April 28 and May 2, 2013. The study population comprised 128 undergraduate students who either participated in the study as part of their program requirements or received a voucher for "Coffee and Pastry" at the university cafeteria for their participation.

5. Results

5.1. Reading a privacy policy

Of the 64 participants in the non-default group who were asked to agree to the terms and conditions of the study without being presented with the policy by default, only 13 (20.3%) clicked the link to read the policy. The remaining 50 participants (79.7%) agreed to the terms without clicking the link to read the policy.

The 64 participants assigned to the default group were presented with a complete copy of the terms and conditions, followed by a request to indicate their agreement by marking the checkbox. Of these participants, the average time spent on the policy page was 59,196.11 ms (median 52,566). This impressive result of close to 1 min on average devoted to reading a 451-word document is encouraging and indicates that the policy was relatively carefully read when presented by default, rather than dismissed lightly.

To test for significance in differences in the time spent on reading the policy between the two study conditions (the default group and the non-default group), a *t*-test for independent groups was conducted. Unsurprisingly, participants in the default condition spent much more time reading the policy ($M = 59196.11$, $SD = 38880.69$) than did participants in the non-default condition ($M = 4905.77$, $SD = 16476.51$), ($t(_{84.92}) = 10.285$, $p < .001$). Cohen's effect size value ($d = 1.82$) suggests a high practical significance. The significant difference between the groups is not surprising, since 50 participants in the non-default condition failed to press the link to read the policy, as a result of which participants in this group devoted an average of only 5 s to reading the policy page.

To compare means only between users who read the policy (participants in the default condition and participants in the non-default condition who clicked the link), a second *t*-test for independent groups was conducted. Results show that participants in the default group devoted much more time to reading the policy ($M = 59196.11$, $SD = 38880.69$) than did the participants in the non-default group who actively pressed the link to read the policy ($M = 24151.46$, $SD = 30359.51$), ($t(_{75}) = -3.06$, $p < .01$). Cohen's effect size value ($d = 1$) suggests a high practical significance. Surprisingly, the participants who clicked on the link spent almost 2.5 times less time on the page than did participants in the default condition.

Time spent on a page does not necessarily mean that participants are reading the policy. To further investigate this finding, we compared participants' eye-tracking measurements for each paragraph in the policy, in both study conditions. In six of the nine paragraphs of the privacy policy, significant differences between the groups were found to support the general finding that participants who were presented with the policy by default, read the document, and most of its paragraphs, much more carefully (in terms of dwell time and fixations) than participants who actively pressed the link to read the policy in the non-default condition. While we might have expected the opposite results, since the participants who pressed the link made a conscious decision to read the policy, these participants in effect devoted significantly less effort in reading the document. Fig. 1 illustrates the differences in reading between participants from both groups who read the statement. Table 1 summarizes the measurements and corresponding paragraphs that were significantly different between the groups, and the *t*-test value for these measures. No significant differences were found between the groups for the remaining paragraphs.

The above findings all support hypothesis H1 by demonstrating that when a privacy policy is presented to participants by default, they spend significantly more time and effort reading it than participants who are asked to indicate their agreement without being presented with the policy by default.

With regard to the first research question-the average time spent on the policy page among all users who read it (including participants from the non-default group who pressed the link) was 53,279.48 ms (just over 53 s).

Further results indicate that participants in both conditions, who read the policy, read the paragraphs in their order of appearance. The average entrance time for each paragraph matches its order in the policy.

Other findings that suggest a comprehensive reading pattern were measured by the number of fixations and average time devoted to each paragraph. These findings clearly show that longer paragraphs were read longer and resulted in more fixations by the participants, with the exception of the introduction (first paragraph), probably due to its location at the beginning of the text and the time readers required to start reading. Table 2 summarizes the average entrance time, dwell time and fixation count for each paragraph, presented alongside to the paragraph's order and size as a percentage of the page size.

The two sets of results together strengthen the assumption that participants who read the policy took time and effort to actually read, rather than merely skim through the policy's text. These findings answer the second research question.

Another interesting and relevant observation relates to the content of paragraphs dwelled and fixated on most by participants, relatively to their size. They all deal with the type of information collected and the authorized and prohibited uses of this information: The dwell time for the paragraph "Information we collect", which describes the ways for collecting information and the kinds of information collected during the experiment, was 120% compared to the paragraph's relative size in the policy's text. The paragraph "How we use your personal information", describing the authorized uses of information collected during the experiment was dwelled on 128% compared to its relative size in the text. And the paragraph "Sharing and disclosure of personal information", setting the rules for sharing the information with third parties was dwelled on 105% compared to its relative size.

5.2. Understanding the restrictions on the use of personal data

We proceeded to examine whether participants in the default group would better understand the permitted and prohibited uses of their data according to the policy compared to participants in the non-default group. More specifically, since participants in the non-default condition spent less time on reading the policy, they consequently should be less likely to know what the policy authorizes and prohibits the researcher with regard to the use of data collected during the study. In other words, dwell time is hypothesized to mediate default/non-default policy presentation and participants' understanding of the policy's principles.

In the post-session questionnaire, participants answered six questions designed to test their knowledge on the authorized and prohibited uses of personal data described in the privacy policy. The questions were simple yes/no questions, presented to participants as follows (percentages of correct answers in parentheses):

1. Does the privacy policy allow the researchers to use the study data for research purposes? (Yes – 70%)

Table 1
Significant differences in measurements of the policy's paragraphs between participants who read the policy in the non-default group and participants in the default group.

Paragraph title	Measurement	Group 1- default group (n = 64)	Group 2- non-default who pressed the link (n = 13)	T Value and significance
Information we collect	Dwell time (ms)	M = 6833.70, SD = 5000.26	M = 3664.12, SD = 5001.50	$t_{(75)} = -2.08^{*}$
Information we collect	Fixation count	M = 22.75, SD = 15.03	M = 11.92, SD = 16.45	$t_{(75)} = -2.32^{*}$
Information we collect	Fixation time (ms)	M = 6538.83, SD = 4847.94	M = 3497.91, SD = 4729.30	$t_{(75)} = -2.07^{*}$
Use of cookies	Dwell time (ms)	M = 2576.80, SD = 1828.72	M = 767, SD = 1012.04	$t_{(30.63)} = -5.00^{***}$
Use of cookies	Fixation count	M = 9.30, SD = 6.07	M = 3.23, SD = 3.88	$t_{(75)} = -3.45^{**}$
Use of cookies	Fixation time (ms)	M = 2484.86, SD = 1791.94	M = 745.82, SD = 980.61	$t_{(31.08)} = -4.94^{***}$
Use of cookies	Dwell time percentage	M = 4.59, SD = 2.56	M = 2.40, SD = 2.55	$t_{(75)} = -2.81^{**}$
Use of cookies	Fixation time percentage	M = 4.41, SD = 2.51	M = 2.34, SD = 2.49	$t_{(75)} = -2.72^{**}$
How we use your personal Information	Dwell time (ms)	M = 5060.44, SD = 4441.98	M = 1870.29, SD = 3623.83	$t_{(75)} = -2.43^{*}$
How we use your personal Information	Fixation count	M = 16.64, SD = 11.99	M = 6.31, SD = 12.15	$t_{(75)} = -2.83^{**}$
How we use your personal Information	Fixation time (ms)	M = 4806.17, SD = 4359.65	M = 1795.71, SD = 3455.94	$t_{(75)} = -2.34^{*}$
Access to your personal data	Dwell time (ms)	M = 3563.13, SD = 3262.10	M = 1292.09, SD = 2536.03	$t_{(75)} = -2.37^{*}$
Access to your personal data	Fixation count	M = 12.89, SD = 10.77	M = 4.69, SD = 8.33	$t_{(75)} = -2.59^{*}$
Access to your personal data	Fixation time (ms)	M = 3402.54, SD = 3145.06	M = 1213.15, SD = 2461.09	$t_{(75)} = -2.36^{*}$
Children under 18	Dwell time (ms)	M = 2573.24, SD = 2632.52	M = 922.39, SD = 1520.02	$t_{(75)} = -2.18^{*}$
Children under 18	Fixation count	M = 9.44, SD = 8.46	M = 3.65, SD = 5.81	$t_{(75)} = -2.37^{*}$
Children under 18	Fixation time (ms)	M = 2438.16, SD = 2527.45	M = 901.07, SD = 1490.58	$t_{(75)} = -2.11^{*}$
Changes to this privacy policy	Dwell time (ms)	2366.54, SD = 2619.19	M = 508.33, SD = 758.14	$t_{(66.39)} = -4.78^{***}$
Changes to this privacy policy	Fixation count	M = 7.72, SD = 7.28	M = 1.85, SD = 2.61	$t_{(54.13)} = -5.05^{***}$
Changes to this privacy policy	Fixation time (ms)	M = 3.73, SD = 3.05	M = 2.13, SD = 3.66	$t_{(68.31)} = -4.91^{***}$

$^{*}p < .05$ $^{**}p < .01$ $^{***}p < .001$.

Table 2
Average entrance time, Dwell time and Fixation Count for each of the policy's paragraphs among the participants who read the policy.

Paragraph	Order of paragraph in the text	Average entrance time (in milliseconds)	Size (in percentage of the total size of the page)	Dwell time (in milliseconds)	Fixation count
Privacy policy (introduction)	1	2537.05	3.03%	3247.41	11.18
Information we collect	2	6091.40	6.27%	6298.57	20.9
Use of cookies	3	14065.67	3.03%	2271.25	8.27
How we use your personal Information	4	18036.74	4.24%	4521.84	14.9
Access to your personal data	5	21647.10	3.89%	3179.71	11.51
Children under 18	6	29245.04	3.43%	2294.51	8.45
Sharing and disclosure of personal information	7	32314.71	7.33%	6401.83	21.86
Securing the information collected	8	43610.07	5.76%	3190.60	11.45
Changes to this privacy policy	9	44567.55	3.07%	2052.81	6.73

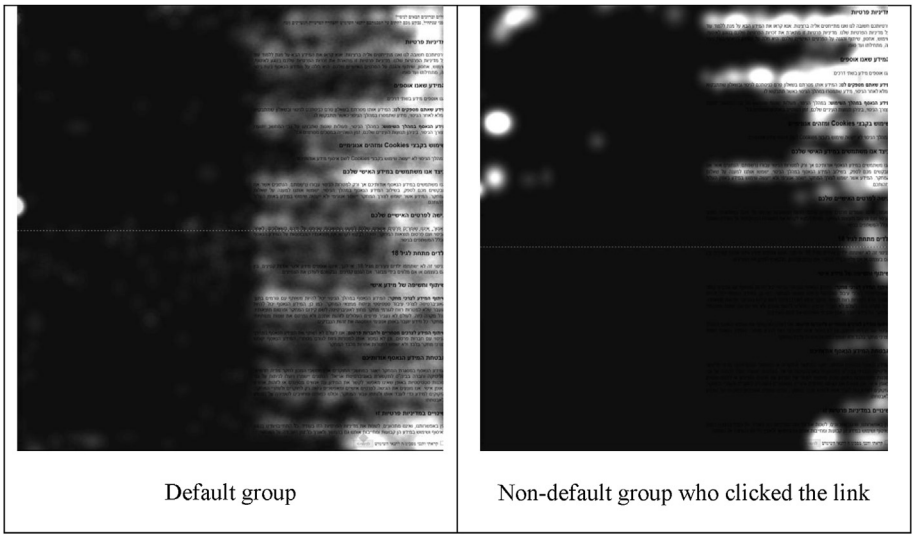

Fig. 1. Focus maps of reading the policy- Among users in the default group, and users in the non-default group who clicked the link to read the policy (The policy is in Hebrew and written right-to-left. Areas where subjects dwelled on are transparent. Level of transparency indicates level of dwelling-more time spent on the area).

2. Does the privacy policy allow the researchers to sell data outside the university for commercial use? (No – 53%)
3. Does the privacy policy allow the researchers to share the study data with others in the university for research purposes? (Yes – 43%)
4. Does the privacy policy allow the researchers to share the study data with others in the university for purposes other than research? (No – 41%)
5. Does the privacy policy allow the researchers to contact you after the study, using the information you provided? (No – 27%)
6. Does the privacy policy allow the researchers to change the privacy policy in the future? (No – 54%)

An index of Data Use Questions was created by summing the number of correct responses to these six items (Cronbach's $\alpha = .76$).

To test if a default policy presentation generates a better understanding of the restrictions imposed on data use, mediated by the time spent on the policy page, regression analyses were performed.

The mediational hypothesis was supported by the results of these tests. The predictor variable (experiment condition: default/non-default) significantly predicted both the outcome variable (Data Use Questions; $R^2 = .11$, $F_{(1,126)} = 15.41$; $\beta = -.33$, $SE = .33$, $p < .001$) and the proposed mediator (duration on policy's page; $R^2 = .46$, $F_{(1,126)} = 105.79$; $\beta = -.68$, $SE = 5278.47$, $p < .001$). Additionally, duration on the policy page significantly predicted Data Use Questions ($R^2 = .14$, $F_{(1,126)} = 21.16$; $\beta = .38$, $SE = .00$, $p < .001$). To test for mediation, a hierarchical regression analysis was conducted with study condition and duration on policy page as predictor variables (using the Enter method, where duration on policy page was entered in step 2) and Data Use Questions as the outcome variable. The overall equation was significant, $R^2 = .15$, $F_{(2,125)} = 11.36$ $p < .001$. Duration on policy page still significantly predicts Data Use Questions even when controlling for study condition ($\beta = .29$, $SE = .00$, $p < .05$), but the relationship between study condition (the predictor) and Data Use Questions (the outcome) becomes insignificant when controlling for duration on policy page ($\beta = -.14$, $SE = .43$, $p =$ n.s). These results suggest full mediation of duration on policy page, and support hypothesis H2: Participants in the default group better understood the permitted and prohibited uses of personal data according to the policy, as a result of spending more time reading the policy than did participants in the non-default group. Fig. 2 summarizes these results.

5.3. Perceived importance of privacy and privacy policies, and reading the policy

In the post-session questionnaire, participants completed several items designed to elicit information on the significance they attribute to privacy and to the availability of privacy policies on websites they visit, in order to test for correlations between perceived significance of privacy or privacy policies, and time devoted to reading the policy. Surprisingly, no correlations were found be-

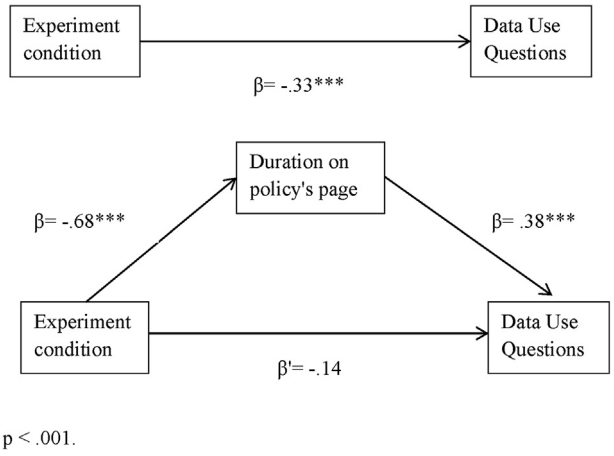

Fig. 2. Model testing hypothesis that duration on policy's page mediates the relationship between experiment condition and data use questions.

tween the privacy-related questions and the time spent on the policy page. Participants who agreed strongly with the statements, "My privacy is important to me" and "I never provide information online unless I have to", participants who reported "Always" or "Sometimes" reading privacy policies of websites they sign up for, and participants who stated they see "great importance" in the existence of privacy policies did not spend significantly more time on the policy page than other participants. Therefore, hypothesis H3 was not supported. Apparently, default presentation of the policy attracted greater attention, independent of participants' position on the importance of privacy. In addition, no gender or socio-economic effects were found on time devoted to reading the policy.

6. Conclusions

Findings of this study indicate that when a website privacy policy is presented to users by default, they will tend to devote significant time and effort to reading it. However, when users have the option of accepting website terms and conditions without reading a policy, they will generally forgo reading the document. Even when users decide to click a non-obligatory link to read the policy, they spend much less time and effort actually reading the document.

One possible explanation for this puzzling finding lies in the act of clicking on the link. It is possible that clicking the link to read the policy, in itself, served as a source of reassurance for users. By clicking the link, participants felt that they had made an active effort to become informed, and having done so they no longer felt the need to actually read the document. The act of clicking the link, which only one-fifth of the participants chose to do, came at the expense of spending time and effort reading the policy, and so even the few who went out of their way and clicked to read the policy ultimately skimmed through the policy text, in comparison to participants who were presented with it by default. This explanation is merely a conjecture and could not be tested with the current data.

Data generated by the eye tracking device add to the basic duration time and allows us to explore **how** the policy has been read by participants. The findings illustrate which paragraphs were read and fixated on most, relatively to their size, suggesting the kind of information that participants found more important or relevant to them in the text-namely paragraphs concerning the kinds of data collected and how it is used by the researcher.

The study further shows that as a result of being presented with the policy by default, which resulted in more time spent on reading the policy, participants better understood their rights and the restrictions on the use of personal data collected during the experiment, as stated by the policy. Increasing user awareness of the potential uses of personal data by the service provider is a social interest, but can also be the interest of service providers, since users who feel they have greater control over their engagement with a website tend to trust the website more and make more informed decisions with regard to their online interactions.

In conclusion, it seems that there are still ways to encourage users to become more aware and informed with regard to the use of personal online data, and that when the cost of being informed is reasonable, users do tend to actively acquire that information.

Informed users are empowered users who can better control their online engagements. They are more confident and believe in their ability to affect how websites and services use the data they collect. They are consumers who have a better chance at influencing the conduct of companies that rely on their customers' disclosure of personal information. The more users read policies, the more they are aware of the way data is used and can demand changes, more transparency and more control. The more users engage with the policy and raise concerns and demands to the company-the greater are the chances for change in service and consideration of users' demands. Nonetheless, with the way privacy policies are being drafted and managed today, it is unreasonable to expect users to actually become informed.

The way we manage our engagement with online services can be improved. We are, in fact, seeing a recent increase in projects promoting standardization of privacy policies, creating universal measurements for "fairness of use" (e.g., TRUSTe, 2015), or projects designed to help users understand the principles of website data use policies (e.g., TosDR), alongside technological innovations aimed at giving users tools to manage and protect their information from abuse by third parties (e.g., Ghostery). The solution cannot be limited merely to making such policies accessible. When policies are drafted in a manner that makes them lengthy and incomprehensible, when the user has no way of affecting the way her data is treated, when policies keep changing constantly, reading the policy will not solve the problem. Nonetheless, for the time being, privacy policies are the common method employed by online services to regulate the use of personal data. A recommendation in an FTC report from 2013 to make privacy policies the standard for mobile applications as well (Federal Trade Commission, 2013), in addition to the short permissions list currently displayed at installation, suggests that this system would not change in the near future. Ensuring that the information is accessible and comprehensible, in a manner that facilitates users' understanding of the principals of their engagement with a website and possibly what they can do to affect the way information about them is treated —is a step forward in the attempt to empower users and equip them with the means to demand and advance fair use of information. This study focused on the factors that promote reading of website privacy policies. The next step is designing ways to make the information clear and facilitate comparisons between websites on the basis of their policies.

Contrary to the pessimistic approach that views compromising and loss of control over personal information as a necessary evil of the information age, this study strengthens the claim that other conduct can be cultivated, and users can be informed of their rights by framing the information differently, specifically by designing website default options involving the presentation of privacy policies. And although companies usually have no incentive to encourage users to read their policies, demands made by users, government officials, activist groups etc. may lead companies to comply and take steps that are less desirable to them, if the im-

plications of not complying may be even less desirable (such as heavy fines for violating privacy laws or users' boycott of a service). A note sent from Facebook to its users regarding changes made to the company's privacy policy in January, 2015, demonstrates this point: "Over the past year, we've introduced new features and controls to help you get more out of Facebook, and listened to people who have asked us to better explain how we get and use information" (Facebook, 2015).

7. Study limitations

Given that the participants in this study are all undergraduate students, we might expect their behavior and awareness of privacy issues and privacy policies to be different from those of the average user. Furthermore, the fact that the privacy policy presented to participants referred to the use of data by researchers in an authorized experiment in their university may have led participants to trust the researchers more than they would a web service. The privacy policy presented to participants was intentionally shorter than the average policy, in order to test for presentation strategy effects only, and eliminate effects of length or complexity of the Policy. With these limitations in mind, given that the two experiment groups were matched and the privacy policies presented to the participants identical in any way, the differences in the conduct of the groups remain relevant and meaningful. The setting of the current study, namely presenting a policy that is accurate, genuine, and relevant for the context in which the participants engaged, was, despite its disadvantages, the best way to simulate a real case of online activity involved in usage of personal data, where a user is asked to sign her agreement to the terms of data use which have actual and immediate relevance to her.

Acknowledgment

The study was supported by the Center for the Study of New Media, Society and Politics at Ariel University. The author thanks Tamar Glauber and Anna Rudaev for their assistance in managing the experiment laboratory and analyzing the data.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 2*, 24–30. http://dx.doi.org/10.1109/MSP.2005.22.

Alexa (2012). *Alexa top 500 global sites* Retrieved from http://www.alexa.com/topsites/global .

Angulo, J., Fischer-Hübner, S., Pulls, T., & Wästlund, E. (2011). Towards usable privacy policy display and management—The primelife approach. In S. M. Furnell, & N. L. Clarke (Eds.), *Proceedings of HAISA 2011: The fifth international symposium on human aspects of information security & assurance* (pp. 108–117). Plymouth: University of Plymouth.

Antón, A. I., Earp, J. B., & Carter, R. (2003). Precluding incongruous behavior by aligning software requirements with security and privacy policies. *Information and Software Technology, 45*(14), 967–977. http://dx.doi.org/10.1016/S0950-5849(03)00095-8.

Ariely, D. (2008). *Predictably irrational: The hidden forces that shape our decisions*. New York: HarperCollins.

BBC (2012, August 9). *Google fined over Safari cookie privacy row* Retrieved from http://www.bbc.co.uk/news/technology-19200279 .

BBC (2013, April 2). *European data watchdogs target Google over privacy*. BBC Online. Retrieved from http://www.bbc.co.uk/news/technology-22003551 .

BBC (2013, February 18). *EU 'may take action' against Google over privacy policy*. BBC Online. Retrieved from http://www.bbc.co.uk/news/technology-21499190 .

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*, 245–270. http://dx.doi.org/10.1016/S0963-8687(02)00018-5.

Bellman, S., Johnson, E. J., & Lohse, G. L. (2001). To opt-in or opt-out? it depends on the question. *Communications of the ACM, 44*(2), 25–27. http://dx.doi.org/10.1145/359205.359241.

Chellel, K., & Hodges, J. (2012, May 19). *Facebook suit over subscriber tracking seeks $15 billion*. Bloomberg Retrieved from http://www.bloomberg.com/news/2012-05-18/facebook-sued-for-15-billion-in-suit-over-user-tracking.html .

Earp, J. B., Antón, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management, 52*(2), 227–237. http://dx.doi.org/10.1109/TEM.2005.844927.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*, 81–83. Facebook (n.d.). Data Policy. Retrieved from https://www.facebook.com/policy.php . http://dx.doi.org/10.1145/641205.641209.

Facebook (2015). *Updating our terms and policies: Helping you understand how Facebook works and how to control your information* Retrieved from https://www.facebook.com/about/terms-updates .

Federal Trade Commission (2013, February). *Mobile privacy disclosures: Building trust through transparency* Retrieved from www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf .

Federal Trade Commission (2000, May). *Privacy Online: Fair Information Practices in the Electronic Marketplace* Retrieved from http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission Ghostery, n.d., http://www.ghostery.com/ .

Goel, V., & Wyatt, E. (2013, September 11). *Facebook privacy change is subject of F.T.C. inquiry*. The New York Times Retrieved from http://www.nytimes.com/2013/09/12/technology/personaltech/ftc-looking-into-facebook-privacy-policy.html Google (n.d.). Privacy Policy. Retrieved from http://www.google.com/policies/privacy/.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *MIS Quarterly, 31*(1), 19–33.

Jentzsch, N., Preibusch, S., & Harasser, A. (2012). *Study on monetising privacy: An economic model for pricing personal information*. Enisa February.

Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: why opting in-opting out. *Marketing Letters, 13*(1), 5–15. http://dx.doi.org/10.1023/A:1015044207315.

Johnson, E. J., & Goldstein, D. (2003). Do defaults save lives? *Science, 302*, 1338–1339. http://dx.doi.org/10.1126/science.1091721.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: the endowment effect, loss aversion, and status quo bias. *The Journal of Economic Perspectives, 5*(1), 193–206.

Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. *American Psychologist, 39*(4), 341–350. http://dx.doi.org/10.1037/0003-066X.39.4.341.

Kesan, J., Hayes, C., & Bashir, M. (2012). Consumer privacy choices, informed consent, and baseline protections to facilitate market transactions in the cloud. *Illinois Program in Law, Behavior and Social Science*, 11–20 Paper No. LBSS12-11.

Korobkin, R. (1998). The status quo bias and contract default rules. *Cornell Law Review, 83*, 608–687.

Kravets, D. (2013, August 26). *Judge approves $20M Facebook 'sponsored stories' settlement*. Wired Retrieved from http://www.wired.com/threatlevel/2013/08/judge-approves-20-million-facebook-sponsored-stories-settlement/ .

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*, 540–565.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations, 4*, 1–17. http://dx.doi.org/10.4018/jeco.2006010101.

Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue. *Journal of Public Policy & Marketing, 19*(1), 1–6. http://dx.doi.org/10.1509/jppm.19.1.1.16934.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29. http://dx.doi.org/10.1002/dir.20009.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48. http://dx.doi.org/10.1162/DAED_a_00113.

Pew Research Center (2012). *Privacy and data management on Mobile devices* Washington, DC: Boyles, J.L., Smith, A., & Madden, M.

Pew Research Center (2013). *Teens and mobile apps privacy* Washington, DC: Madden, M., Lenhart, A., Cortesi, S., & Gasser, U.

Pew Research Center (2015). *Americans' privacy strategies post-snowden* Washington, DC: Rainie, L., & Madden, M.

Pfanner, E. (2012, February 29). *France says Google privacy plan likely violates European law*. The New York Times Retrieved from http://www.nytimes.com/2012/02/29/technology/france-says-google-privacy-plan-likely-violates-european-law.html .

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*, 27–41. http://dx.doi.org/10.1509/jppm.19.1.27.16941.

Rosenblatt, J. (2012, October 5). *Facebook seeks dismissal of $15 billion privacy suit*. Bloomberg Retrieved from http://www.bloomberg.com/news/2012-10-05/facebook-seeks-dismissal-of-15-billion-privacy-suit.html .

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty, 1*, 7–59. http://dx.doi.org/10.1007/BF00055564.

Seshagiri, A. (2013, October 1). *Claims that Google violates Gmail user privacy*. The New York Times Retrieved from http://www.nytimes.com/interactive/2013/10/02/technology/google-email- case.html SMI (n.d.). RED-M. Retrieved from http://www.smivision.com/en/gaze-and-eye-tracking-systems/products/redm.html.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press Terms Of Service; Didn't READ (n.d.) http://tosdr.org .

TRUSTe (n.d.)2015 http://www.truste.com.
Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: an experimental study. *Information Systems Research*, *22*, 254–268.
Womack, B. (2013, August 29). *Facebook seeks to clarify how it uses member data for ads*. Bloomberg Retrieved from http://www.bloomberg.com/news/2013-08-29/facebook-seeks-to-clarify-how-it-uses-member-data-for-ads.html .