

# “Now that you mention it”: A Survey Experiment on Information, Salience and Online Privacy

Helia Marreiros<sup>a</sup>, Mirco Tonin<sup>b</sup>, Michael Vlassopoulos<sup>a</sup>, m.c. schraefel<sup>c</sup>.

January 2016

Personal data lie at the forefront of different business models and constitute the main source of revenue of several online companies. In many cases, consumers have incomplete information about the digital transactions of their data. This paper investigates whether highlighting positive or negative aspects of online privacy, thereby mitigating the informational problem, can affect consumers' privacy actions and attitudes. Results of two online survey experiments indicate that participants adopt a more conservative stance on disclosing identifiable information, such as name and email, even when they are informed about positive attitudes of companies towards their privacy. On the other hand, they do not change their attitudes and social actions towards privacy. These findings suggest that privacy concerns are dormant and may manifest when consumers are asked to think about privacy; and that privacy behavior is not necessarily sensitive to exposure to objective threats or benefits of disclosing personal information.

*JEL classification: C83, L38, M38*

Keywords: survey experiment; information economics; privacy policies; salience; self-disclosure

---

<sup>a</sup> University of Southampton, Economics Department, School of Social Sciences, SO17 1BJ Southampton, UK. Corresponding author: [h.marreiros@soton.ac.uk](mailto:h.marreiros@soton.ac.uk). Tel: +442380599328

<sup>b</sup> Free University of Bolzano, Faculty of Economics and Management, 39100, Bolzano, Italy; IZA, Bonn; CESifo, Munich; Dondena, Milan.

<sup>c</sup> University of Southampton, Electronics and Computer Sciences Department, SO17 1BJ Southampton, UK.

We acknowledge financial support from Research Councils UK via the Meaningful Consent in the Digital Economy Project - grant reference EP/K039989/1. We are grateful for the feedback from participants of the Workshop on Meaningful Consent on the Digital Economy – MCDE 2015.

## 1. Introduction

Agreeing with the terms and conditions and privacy policies of online service providers has become a daily task for billions of people worldwide.<sup>1</sup> By ticking the consent box, online consumers usually give permission to service providers to collect, share or trade their personal data in exchange for various online services. Indeed, personal data lie at the forefront of different business models and constitute an important source of revenue for several online companies, such as Google and its subsidiary DoubleClick, and Amazon (Casadesus-Masanell and Hervas-Drane 2015). Despite giving formal consent, consumers are often unaware of what these digital transactions involve (Acquisti et al. 2015b, Beresford et al. 2012) and have incomplete information about the consequences of disclosing personal information - when, how and why their data are going to be collected and with whom these data are going to be traded (Acquisti and Grossklags 2005b, Vila et al. 2003). A considerable number of studies (Acquisti 2004, Acquisti and Grossklags 2005a, Acquisti et al. 2015a, Brandimarte and Acquisti 2012, Chellappa and Sin 2005, Jensen et al. 2005, Norberg et al. 2007) and consumer surveys show that consumers are generally concerned about privacy,<sup>2</sup> while the issue of privacy regulation has entered the policy agenda with important challenges being raised, for instance, regarding the scope of government surveillance and the legal framework surrounding data sharing.<sup>3</sup> For instance, reforming data protection rules in the EU is currently a policy priority for the European Commission.<sup>4</sup> At the same time, some online companies (e.g. the search engine DuckDuckGo) use enhanced privacy as a way of differentiating their product (Tsai et al. 2011), or even build their business model around the protection of privacy (e.g. Disconnect.me).

The economics approach to privacy posits that consumers make disclosure decisions considering the benefits and costs associated with revealing personal information (e.g. Acquisti et al. 2015b, Posner 1981, Stigler 1980, Varian 1997). Each time consumers face a request to disclose personal information to service providers, they process the available information and decide accordingly by evaluating the risks and benefits of this exchange (Chellappa and Sin 2005, Culnan 1993, Culnan and Armstrong 1999, Dinev and Hart 2006, Hann et al. 2008,

---

<sup>1</sup> As of the third quarter of 2015, Facebook had 1.55 billion monthly active users. <http://newsroom.fb.com/company-info/>

<sup>2</sup> For instance, 72% of US consumers revealed concerns with online tracking and behavioral profiling by companies – Consumer-Union 2008 – (<http://consumersunion.org/news/poll-consumers-concerned-about-internet-privacy/>).

<sup>3</sup> The interaction between privacy protection regulation and market performance and structure is analyzed in Campbell et al. (2015), Goldfarb and Tucker (2011) and Shy and Stenbacka (2015).

<sup>4</sup> In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. The completion of this reform was a policy priority for 2015. On 15 December 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules, establishing a modern and harmonized data protection framework across the EU. [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)

Hui and Png 2006, Milne and Rohm 2000, Xu et al. 2010). Sharing personal information provides consumers with benefits that are tangible (e.g. free access to online services, personalized ads, discounts) and intangible (e.g. the possibility to connect with long-lost friends), but also gives rise to potential costs (e.g. risk of identity theft, shame of exposure of personal information, potential exposure to price discrimination, being bothered by an excessive volume of ads).<sup>5</sup> While consumers may be aware of the many benefits of disclosing personal information, the potential costs are not so clear. There is evidence that consumers tend to disclose their personal information most of the time (Acquisti and Grossklags 2012, Adjerid et al. 2013, 2014, Beresford et al. 2012, Goldfarb and Tucker 2012, Olivero and Lunt 2004); yet it is questionable whether this is due to the benefits of disclosure generally being considered greater than the associated costs - that is, whether this is an informed and rational choice. To start with, consumers may fail to fully inform themselves, even if the relevant information is readily available. Indeed, although users mechanically accept the terms and conditions by ticking a box, few read the privacy policies (Jensen and Potts 2004, Privacy Leadership Initiative 2001, TRUSTe 2006) and those who do try to read them find them time-consuming and difficult to understand (McDonald and Cranor 2008, Turow et al. 2005). Moreover, there is growing evidence emerging from the various behavioral sciences that several behavioral biases and heuristics influence individuals' choices regarding sharing personal information online (e.g. Acquisti and Grossklags 2005a, 2007, Acquisti et al. 2013, 2015b, Baddeley 2011).

What we study in this paper is whether users' privacy decisions are influenced by exposure to information about the threats and benefits associated with disclosing personal information online. In particular, we investigate whether information has an impact on disclosure actions and on privacy attitudes, as well as on social actions. Becoming more aware of the threats associated with disclosure of personal information could influence consumers to change their own individual behavior - for instance by withholding information, but it could also lead to an increased pressure on policy makers to take action - for instance, by implementing more consumer-friendly regulations. In the language of Hirschman (1970), a consumer could react to information about threats to online privacy by "exit" (withholding their own information) or "voice" (asking for more protection for all users), or both. To the best of our knowledge, this is the first paper to investigate both these aspects. In light of

---

<sup>5</sup> The three main benefits of the privacy tradeoff identified in the privacy literature are financial rewards, such as discounts (Caudill and Murphy 2000, Hann et al. 2008, Phelps et al., 2000, Xu et al. 2010), personalization and customization of information content (Chellappa and Shivendu 2010, Chellappa and Sin 2005). See also Acquisti (2015b) for an overview of the cost and benefits of sharing information for both data holders and data subjects.

the regulatory activism highlighted above, the effect of information on public opinion and on the willingness to engage in social actions is particularly relevant.

In two separate survey experiments we explore two potential sources of information regarding privacy - privacy policies and news reports. While terms and conditions are obviously available to consumers who are asked to accept them, the information they include is often not easily accessible due to the excessive length and obscure language of the documentation. What would happen if these informational problems were mitigated by clearer and more readable privacy policies? Moreover, as privacy-related stories attract more headlines in mainstream media,<sup>6</sup> an interesting question is how people react to this. Thus, we also investigate whether news coverage of actual privacy practices by companies affects users' privacy preferences. To address these questions, we conducted two online survey experiments, with over 1000 respondents, involving two types of informational intervention. In the first experiment, we study how informing participants about specific statements taken from Facebook and Google privacy policies - and rated in a pre-test as reflecting either a positive, negative or neutral attitude towards their users - affects individuals' concerns and behavior in relation to online privacy. In the second study, we use extracts from newspaper articles related to privacy practices of companies like Facebook and Dropbox and ask whether exposure to these shifts users' privacy concerns.

Our experimental design involves three treatments. Participants are randomly presented with a statement from a company's privacy policy that highlights either a positive, a negative or a neutral attitude toward users (experiment one) or with a newspaper article extract highlighting a positive, neutral or negative privacy practice (experiment two). We then collect three measures of participants' privacy concerns: a) actual propensity to disclose personal information (e.g. name, email) in a demographic web-based questionnaire that we administered; b) participation in a social action: whether users vote for a donation to be made to a privacy advocacy group or to an alternative, not privacy-related, group; and c) stated attitudes toward privacy and personalization elicited through a survey. Thus, we measure both privacy stated preferences and private and social actions related to privacy.

---

<sup>6</sup> As of 26 Jan 2016, there are 2,170,000 hits in Google news category for the search "online privacy". For instance, The Guardian reported about Londoners giving up their eldest children in exchange for access to public Wi-Fi (<http://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause>), or about Facebook tracking its users, violating UE data protection laws. (<http://www.theguardian.com/technology/2015/mar/31/facebook-tracks-all-visitors-breaching-eu-law-report>). Also, the NYtimes reported about the hidden option of opting out of personalized ads ([http://www.nytimes.com/2015/12/21/business/media/key-to-opting-out-of-personalized-ads-hidden-in-plain-view.html?\\_r=](http://www.nytimes.com/2015/12/21/business/media/key-to-opting-out-of-personalized-ads-hidden-in-plain-view.html?_r=)).

Previous survey evidence suggests an impact of privacy risks on privacy concerns and on intentions to sharing personal data (Dinev and Hart 2006, Malhotra et al. 2004). We therefore expect that, in our survey, highlighting positive (negative) features of the privacy tradeoff will make participants less (more) concerned about privacy and we expect this to be reflected in people's attitudes toward privacy and their willingness to engage in social action promoting privacy protection. This may be either because participants were previously unaware of the benefits and costs that are being presented or because being reminded about them makes them more salient. Saliency may also affect participants' willingness to disclose personal information.

We find that the propensity of some participants to disclose sensitive information (such as name, or email) falls when they are exposed to information regarding privacy. Surprisingly, this is true even when the aspect of privacy they read about relates to positive attitudes of the companies towards their users. Just mentioning the presence of privacy issues, such as the assurance that data are not shared without users' consent or that companies are adopting practices to protect users' data, decreases self-disclosure. This suggests that privacy concerns are dormant and may manifest when users are asked to think about privacy; and that privacy behavior is not necessarily sensitive to exposure to objective threats or benefits of personal information disclosure. The finding of a connection between the salience of privacy and the willingness to divulge personal information is consistent with previous findings (Benndorf et al. 2015, John et al. 2011) that contextual cues do have an impact on levels of disclosure. However, we do not find any effect on social actions, nor on privacy attitudes. In the privacy literature, the disconnect between attitudes and actions - the so-called privacy paradox - is well documented (e.g. Norberg et al. 2007), while we are not aware of previous work demonstrating a disconnect between private and social actions (or, more generally, investigating social actions related to privacy).

The rest of the paper is structured as follows. Section 2 describes the experimental design along with the procedures. Section 3 presents the results and section 4 offers some conclusions. Appendix A contains some additional results.

## **2. Experimental Design and Sample**

To understand the effect of highlighting positive and negative aspects of online privacy on the behavior of online users, we designed two similar online survey experiments. We recruited a total of 1162 paid participants between March and June 2015, using Prolific Academic, a UK-based crowdsourcing community that recruits participants

for academic purposes.<sup>7</sup> Specifically, we recruited 654 participants for the first survey (in two waves) and 508 participants for the second one (in two waves). In both experiments the recruitment was restricted to participants born in the UK, the US, Ireland, Australia and Canada, and whose first language was English. The experiments were designed in Qualtrics Online Sample, and the randomization of treatments was programmed in the survey software.<sup>8</sup>

## **2.1. Experimental Manipulations**

In the first experiment, we used Facebook and Google’s privacy policy statements as experimental manipulations. In the second survey, we used extracts from newspaper articles. These privacy policy statements and news extracts provided information that highlighted a positive, a negative or a neutral aspect of the company’s privacy policy and were selected through a pre-test, where for each study we asked 100 students to evaluate the privacy policies’ statements and the news extracts.<sup>9</sup>

In particular, for the negative treatment in the first experiment, we selected a statement from Facebook’s data policy highlighting how Facebook can share personal information within the family of companies that are part of Facebook. For the positive treatment we selected a statement from Google’s privacy policy, indicating that Google does not share users’ data unless they give their consent, while for the neutral treatment we collected a statement from Facebook’s data policy defining the term “cookies.” In the second experiment, for the negative treatment we selected a news extract on how Facebook is making money by selling unidentifiable data of their users; and for the positive treatment an article on how Dropbox and Microsoft adopt privacy norms that safeguard users’ cloud data (ISO 27018 standard). Finally, for the neutral treatment we selected an article that refers to the health benefits of wearable tech, and is therefore unrelated to privacy issues.<sup>10</sup>

We use a between-subject design, where each participant is exposed to only one treatment - i.e. is exposed to only one of the statements - before we measure privacy preferences. To further validate our experimental manipulation, at the end we asked participants to classify the three statements that were part of their experiment as positive, negative or neutral, in terms of the attitude they revealed vis-à-vis users’ privacy.

## **2.2. Measures of Privacy Preferences**

---

<sup>7</sup> More information about the platform is available at [www.prolific.ac](http://www.prolific.ac)

<sup>8</sup> The surveys are available as supplementary material.

<sup>9</sup> See Marreiros et al. (2015) for the pre-test results of privacy policy statements.

<sup>10</sup>A transcription of the privacy policies’ statements and news extract can be found in appendix B.

First, participants were shown a brief study description, which mentioned that the study was about online privacy, that data collection was subject to the Data Protection Act, and that The University of Southampton ethics committee had approved the study. We then proceeded to evaluate the effect of our experimental manipulation on three measures of privacy preferences:

- 1) disclosure of personal information;
- 2) participation in a social action – voting to allocate a donation to a foundation that protects digital rights or to an unrelated foundation;
- 3) attitudes towards privacy and personalization.

For the first measure, designed to test the impact of the experimental manipulation on *self-disclosure*, participants were initially asked to carefully read one of the statements that are part of our experimental manipulation and indicate whether they had previous knowledge of it. Then, they were asked to reply to 15 demographic and personal questions, covering more or less sensitive information, like gender, income, weekly expenditure, and personal debt situation.<sup>11</sup> The answer to the first 13 questions had to be provided through a scroll-down menu that included the option “Prefer not to say”, so that the effort required to answer was the same as the effort required not to answer. Participants could not proceed without selecting an option from the menu. Notice that providing false information could potentially be an alternative way to preserve privacy. Prolific Academic independently collected some demographic information when participants first registered with the service. Comparing our data to the demographic data collected by Prolific Academic for age, gender and country of residence, we did not find significant differences, thus indicating that lying is not common (see table 8A in appendix A for detailed information). To verify whether participants read the questions carefully, we also included a control question (“This is a control question. Could you please skip this question?”), with a “normal” scroll-down menu (including numbers from 1 to 4 and the option “Prefer not to say”). The last two questions, which were first name and email, were not mandatory.<sup>12</sup>

Regarding the second measure of privacy preferences, *contribution to a social action*, participants were first asked to read the very same statement they had seen earlier and indicate whether they thought that their friends knew about it. The purpose of this was to re-establish the saliency of the provided information. We then asked

---

<sup>11</sup> Typically, more personally defining or identifying items, such as name, or financial or medical data are perceived as more sensitive (Goldfarb and Tucker 2012, Malheiros et al. 2013).

<sup>12</sup> The stage introduction read as follows: “Please provide some information about yourself. Note that you can choose not to provide the information by choosing the option “Prefer not to say.” This option is available in all the mandatory questions of this section.”

participants to choose which institution should receive a donation of £100 from us: EFF - Electronic Frontier Foundation (an organization that fights for online rights and, therefore, is concerned with privacy issues) or Transparency International (an organization that fights against corruption and is therefore unrelated to privacy issues). In particular, participants were informed that *“We are donating £100 to charity. (~ \$154 | ~135€). You can choose which organization we donate the money to: EFF (Electronic Frontier Foundation) or Transparency international. Please note that the institution that receives more votes will be the one receiving the donation”*, and then were provided with a description of the two organizations.<sup>13,14</sup>

Finally, for the third measure of privacy preferences, the one regarding *attitudes*, we started by asking participants to read the statement one more time and indicate whether they thought that society in general knew about it. Again, this question had the purpose of maintaining the salience of the information. We then asked them to take the survey developed by Chellappa and Sin (2005) that evaluates their concern level about online privacy, how much they value personalization, and the likelihood of providing personal information.

After the experiment, participants were asked to answer some more questions. First, to control for the effectiveness of the manipulation, they were asked to evaluate the extent to which the three statements used in the experiment revealed a positive, negative or neutral attitude of Google/Facebook towards their users. Second, we asked some optional miscellaneous questions related to online privacy and the experiment, e.g. whether participants usually read privacy policies or already knew of the two non-profit organizations. Finally, there was a section related to another study, eliciting valuation for apps permissions.

In the second experiment, immediately after the survey measuring attitudes, we also added a demographic questionnaire asking some sensitive and intrusive questions structured in the same way as the initial questionnaire. For instance, we asked information on the number and gender mix of sexual partners, passport number, name of first pet, and mother’s maiden name. Some of these questions are commonly asked to recover passwords and could therefore be seen as very privacy-intrusive. When asking to classify the three news extracts as positive, negative or neutral, we also asked if participants were more or less willing to share their personal data online after reading these extracts. Moreover, we added a final survey about online privacy

---

<sup>13</sup> “EFF (Electronic Frontier Foundation) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development.” <https://www.eff.org>

<sup>14</sup> “Transparency international has as a mission to stop corruption and promote transparency, accountability and integrity at all levels and across all sectors of society. Their Core Values are: transparency, accountability, integrity, solidarity, courage, justice and democracy.” <http://www.transparency.org>



concerns (Buchanan et al. 2007); our decision to include this was based on the fact that it is designed exclusively to evaluate privacy concerns, contrasting with the Chellappa and Sin survey which, besides evaluating privacy concerns, also evaluates the value of personalization and the likelihood of disclosing information. Finally, we asked some optional miscellaneous questions related to online privacy and the study.

### **2.3. Characterization of the Subject Pool**

Our final sample consists of 1075 participants - 600 for the first experiment, 475 for the second one.<sup>15</sup> In the first experiment, 52% of the participants were female and the average age was 28, with 77% part of the “millennial generation” (i.e. born between 1982 and 2004: Howe and Strauss 2000). Most of the participants were from the UK, 69%, or the US, 24%; 85% were white and 58% were students; 70% had two to four years of college education; and 85% had an income lower than 40.000 (in local currency). The average time to complete the survey was nine minutes (see table 1A in appendix A for more detailed descriptive statistics). These characteristics are balanced across the three treatments.

In the second experiment, 47% of the participants were female. The average age was 28 years old (80% part of the “millennial generation”), with 27% of the participants from the UK and 63% from the US; 81% were white, 45% were students, and 73% had a college degree, while 70% had an income lower than 40.000 (in local currency). The average time taken to complete the survey was 13 minutes (see table 2A in appendix A for more detailed descriptive statistics). Also in this case, these characteristics are balanced across the three treatments. Comparing across experiments, the subject pool had similar characteristics, with the exception of the country that participants were born in.

## **3. Results**

Here we present the results for each of our three privacy measures. Before doing so, we checked whether our experimental manipulation was successful. To do this, we exploited the fact that at the end of each experiment we asked participants to classify the three statements used in that experiment as representing a positive, negative or neutral attitude of the service provider towards its users. What we found is that in the first (second) experiment, 85% (84%) of the participants considered that the statement chosen for the positive treatment indeed

---

<sup>15</sup> Out of the initial 1162 participants, we rejected 87 submissions in total: 15 submissions from those that fail the control question (which asked to skip that question) and 72 submissions from those that completed the survey in less than 4 minutes in experiment ‘one’ and in less than 6 minutes in experiment ‘two’. The aim is to exclude those who did not take the task seriously, not reading the questions or doing it extremely quickly. Indeed, in a pilot study with students from The University of Southampton the minimum amount of time per participation was 4.5 minutes and 6 minutes for the two experiments respectively. The time for experiment ‘Two’ was higher than for experiment ‘One’, as it contains additional modules. Rejections did not differ significantly by treatment (chi2 p-value>0.4). Moreover, we find similar results running the analysis with the full sample.

reflected a positive attitude; 77% (92%) of the participants classified the statement chosen for the negative treatment as negative; and 73% (59%) of the participants classified the statement chosen for the neutral treatment as neutral (see table 3A in appendix A for more details).<sup>16</sup> Thus, the majority of the participants classified correctly the statement or news extract after being presented with it, i.e., those that participated in the positive (negative, neutral) treatment classified the statement chosen for that treatment as positive (negative, neutral).

### 3.1. Self-disclosure

We created three variables measuring self-disclosure, all taking the values 0/1:

1. Disclosure-Index: equals 1 if the participant discloses personal information in all the first 13 items of the demographic questionnaire;<sup>17</sup>
2. Give Name: equals 1 if the participant discloses their first name;
3. Give Email: equals 1 if the participant discloses their email address.

For the first experiment, the upper part of Table 1 shows that the large majority of participants (77%) disclosed all the personal information that could not directly identify them as individuals.<sup>18</sup> This result is consistent with previous studies about privacy disclosure (see for example Beresford et al. 2012, Goldfarb and Tucker 2012). However, there was significantly lower disclosure of the information that could identify them as individuals, such as name (only 45% provided their first name) and email (only 31% disclosed their email address). With the exception of three participants, those who disclosed email also disclosed name. We did not find significant differences across treatments;<sup>19</sup> thus it does not seem to be the case that providing “negative” information makes participants more reluctant to disclose private information.

The lower part of Table 1 indicates that 84% of participants disclose all the non-identifiable information in the second experiment, with 50% disclosing their name and 37% their email. Here, in contrast to the first experiment, we found significant differences in the disclosure of identifiable information (Give-Name and Give-Email), with a higher incidence of disclosure of name and email in the neutral treatment compared to the negative and positive treatments.

---

<sup>16</sup> The neutral statement is less frequently recognized as such because of the possibility of deviating in two directions.

<sup>17</sup> Age, health situation, marital status, education, number of times moved house, gender, number of children, number of credit cards, debt situation, country live in, maximum relationship length, annual income, money spent per week.

<sup>18</sup> See table 4A in appendix A for a full description of the percentages of the use of the option “prefer not to say” per variable and per treatment.

<sup>19</sup>(Chi2 test: Positive – Negative: Disclosure index: p-value=0.330; Give-name: 0.410; Give-email: 0.290; Negative-Neutral: Disclosure index: p-value=0.159; Give-name: 0.710; Give-email: 0.891; Neutral – Positive: Disclosure index: p-value=0.673; Give-name: 0.627; Give-email: 0.345).

These results are confirmed in a regression analysis (Table 2 for the first experiment and Table 3 for the second experiment), where we estimate OLS regressions for each of three measures of disclosure on a set of treatment dummies, plus a dummy controlling for recruitment wave. Including - or not including - individual characteristics (age, gender, nationality, ethnicity, student and work status, education level and annual income level) does not change the outcome. Our results indicate that less wealthy individuals and white people are more likely to disclose personal information (for details, see tables 14A and 15A in appendix A). The results on the relationship between wealth and self-disclosure are consistent with those of Goldfarb and Tucker (2012). Also, including a dummy controlling for previous awareness of the information we provide gives similar results (for summary statistics of awareness see tables 9A to 11A in appendix A).

As mentioned in the previous section, in the second experiment we added a module with particularly sensitive questions, where as before participants could disclose information or choose the option ‘prefer not to say.’ We included 11 items: religious (yes or no), race, number of sexual partners, number of serious relations, partner’s gender, weight, high school name, passport number, name of first pet, mother’s maiden name, and favorite place. Compared to the demographic questionnaire, participants were more reluctant to disclose sensitive information. For instance, nobody disclosed passport number and 86% did not disclose mother’s maiden name. Nevertheless, many participants disclosed information for sensitive items; for instance 81% disclosed the number of sexual partners (see table 12A for non-disclosure percentages per variable and per treatment).

To analyze treatment effects, for each of the 11 items, we created a dummy variable that takes the value of 1 if the information is provided and 0 otherwise. We then summated these dummies to create a summary variable called Disclosure-index-SQ that can take values between 0 (if no information is provided) and 11 (if information is provided for all 11 questions). Figure 1 shows a histogram with the distribution of this index by treatment and in total<sup>20</sup>. We can see that the distribution for the neutral treatments is shifted towards higher values, i.e. more disclosure. Mann-Whitney tests confirm that there is indeed a significant difference between the negative and the neutral treatments (p-value=0.011) and between the positive and the neutral treatments (p-value=0.025), while we found no differences between the positive and the negative ones (p-value=0.979). This result is also confirmed in a regression framework, with and without controls for individual characteristics (see table 16A in appendix A).

---

<sup>20</sup> Four participants did not choose the option “prefer not to say” for the passport item, as they made some comments, such as “I don’t have one” or “I don’t understand the reasons to ask for my passport number”. We consider this as a form of non-disclosure.

What is the interpretation of these results? Participants do not seem to react in the predicted way, with positive information inducing more disclosure and negative information increasing their concern for privacy. The fact that in the second experiment participants disclosed more information in the neutral treatment, where privacy was not mentioned, than in the other treatments may suggest that the saliency of privacy issues has an effect on individual online behavior, decreasing self-disclosure. In other words, as in Joinson et al. (2008), just mentioning privacy focusses people`s minds on the issue and induces them to disclose less information. Notice, however, that Joinson et al.`s (2008) study simply primes participants with a survey, while we distinguish between positive and negative information and show that disclosure is reduced even if the information is positive from the point of view of the protection of privacy. Looking at the two experiments together (Table 4), it is indeed evident that disclosure is lower whenever privacy issues are involved, compared to the only case (the neutral treatment in the second experiment) where there is no connection to it, as the information provided referred to the advantages of wearable tech.

**Table 1 Self-disclosure stage**

	<b>Experiment 'One'</b>										
	<b>All</b>		<b>Positive treatment</b>		<i>Pos - Neg</i>	<b>Negative treatment</b>		<i>Neg - Neu</i>	<b>Neutral treatment</b>		<i>Neu - Pos</i>
	N	% "DIS"	N	% "DIS"	p-value	N	% "DIS"	p-value	N	% "DIS"	p-value
Diclosure_Index	600	77%	194	77%	0.330	198	81%	0.159	208	75%	0.673
Give Name	600	45%	194	43%	0.410	198	47%	0.719	208	45%	0.627
Give Email	600	31%	194	28%	0.290	198	33%	0.891	208	33%	0.345

	<b>Experiment 'Two'</b>										
	<b>All</b>		<b>Positive treatment</b>		<i>Pos - Neg</i>	<b>Negative treatment</b>		<i>Neg - Neu</i>	<b>Neutral treatment</b>		<i>Neu - Pos</i>
	N	% "DIS"	N	% "DIS"	p-value	N	% "DIS"	p-value	N	% "DIS"	p-value
Diclosure_Index	475	84%	154	81%	0.146	163	87%	0.291	158	83%	0.688
Give Name	475	50%	154	45%	0.664	163	47%	0.028**	158	59%	0.009***
Give Email	475	37%	154	31%	0.709	163	33%	0.012**	158	47%	0.005***

Disclosure-Index: disclose the information in all the items was scored as '1' and use of the option "prefer not to say" in any of the 13 items was scored as '0'. Give Name and Give Email: disclose the information was scored as '1'.

% DIS: Percentage of participants that disclosed the information.

P-values of pairwise chi2 test on treatment differences: \* p<0.10, \*\* p<0.05, \*\*\* p<0.01.

**Table 2 Regressions on self-disclosure - Experiment ‘one’**

	Disclosure-Index		Give-Name		Give-Email	
	[1]	[2]	[3]	[4]	[5]	[6]
Positive treatment	0.018 (0.04)	0.025 (0.03)	-0.026 (0.05)	-0.027 (0.05)	-0.045 (0.05)	-0.044 (0.05)
Negative treatment	0.058 (0.04)	0.043 (0.03)	0.020 (0.05)	0.009 (0.05)	0.008 (0.05)	0.004 (0.05)
Constant	0.745*** (0.04)	0.062 (0.10)	0.545*** (0.04)	0.242 (0.15)	0.409*** (0.04)	0.117 (0.15)
Individual characteristics	No	Yes	No	Yes	No	Yes
N	600	579	600	579	600	579
R-sqr	0.004	0.383	0.032	0.096	0.030	0.077

Robust standard errors in parentheses.

\* p<0.10, \*\* p<0.05, \*\*\* p<0.01.

Dependent variables: Disclosure-Index - disclose the information in all the 13 items was scored as ‘1’; Give Name and Give Email - disclose the information was scored as ‘1’.

In all the models we control for recruitment wave. Individual characteristics refer to demographic characteristics as age, gender, nationality (UK or US) ethnicity (white or not) Student and work status, education and income (see table 14A in appendix A for coefficients and significance level of the individual characteristics).

**Table 3 Regressions on self-disclosure - Experiment ‘two’**

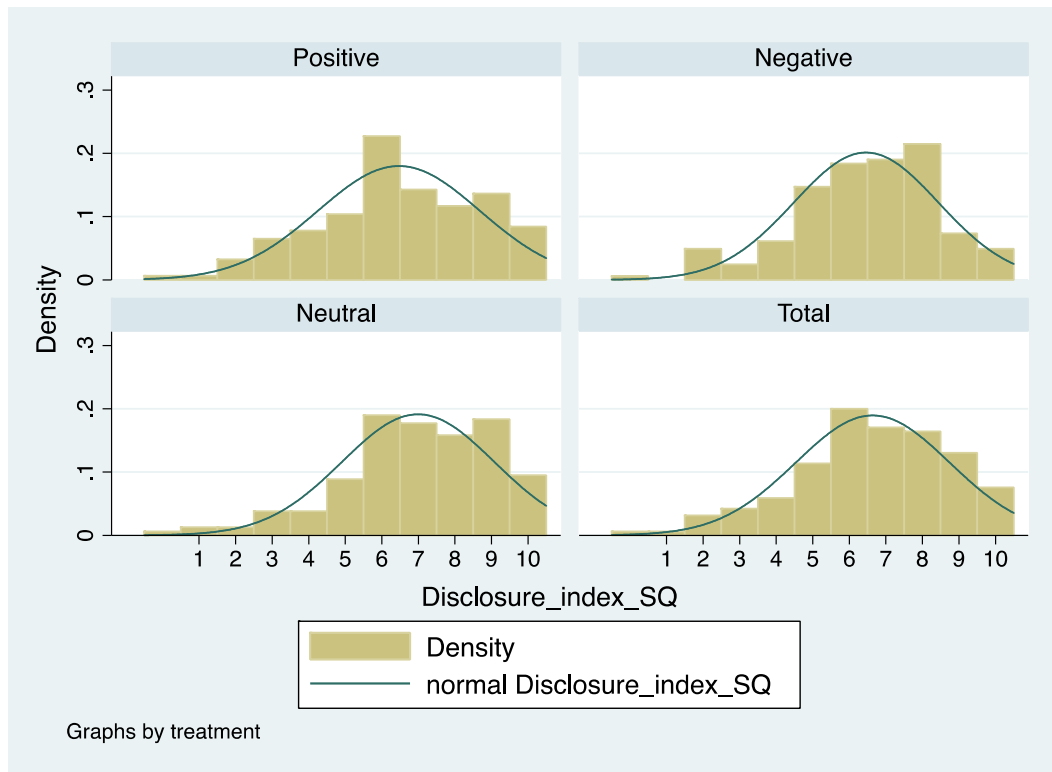
	Disclosure-Index		Give Name		Give Email	
	[1]	[2]	[3]	[4]	[5]	[6]
Positive treatment	-0.018 (0.04)	0.001 (0.04)	-0.148*** (0.06)	-0.156*** (0.06)	-0.157*** (0.05)	-0.140** (0.06)
Negative treatment	0.042 (0.04)	0.053 (0.03)	-0.123** (0.06)	-0.111** (0.06)	-0.137** (0.05)	-0.132** (0.06)
Constant	0.833*** (0.04)	0.142 (0.09)	0.637*** (0.04)	0.434*** (0.15)	0.482*** (0.04)	0.566*** (0.15)
Individual characteristics	No	Yes	No	Yes	No	Yes
N	475	465	475	465	475	465
R-sqr	0.005	0.291	0.025	0.092	0.022	0.062

Robust standard errors in parentheses.

\* p<0.10, \*\* p<0.05, \*\*\* p<0.01

In all the models we control for recruitment wave. Individual characteristics are the same as in the previous table (see table 15A in appendix A for coefficients and significance level of the individual characteristics).

**Figure 1 Histogram of the disclosure of sensitive items**



**Table 4 Effect of privacy awareness on disclosure of information**

		Disclosure-Index		Give Name		Give Email	
		[1]	[2]	[3]	[4]	[5]	[6]
Positive	Exp	-0.061	-0.032	-0.167***	-0.136**	-0.185***	-0.158***
		(0.04)	(0.04)	(0.05)	(0.06)	(0.05)	(0.05)
Positive	Exp	-0.017	-0.000	-0.147***	-0.133**	-0.157***	-0.141**
		(0.04)	(0.04)	(0.06)	(0.06)	(0.05)	(0.06)
Negative	Exp	-0.021	-0.011	-0.125**	-0.116**	-0.135***	-0.119**
		(0.04)	(0.04)	(0.05)	(0.06)	(0.05)	(0.05)
Negative	Exp	0.042	0.044	-0.123**	-0.099*	-0.137**	-0.130**
		(0.04)	(0.04)	(0.06)	(0.06)	(0.05)	(0.05)
Neutral	Exp	-0.079*	-0.056	-0.143***	-0.113**	-0.141***	-0.119**
		(0.04)	(0.04)	(0.05)	(0.06)	(0.05)	(0.05)
Constant		0.829***	0.140*	0.595***	0.387***	0.468***	0.385***
		(0.03)	(0.07)	(0.04)	(0.11)	(0.04)	(0.11)
Individual characteristics	No	Yes	No	Yes	No	Yes	
N	1075	1044	1075	1044	1075	1044	
R-sqr	0.010	0.318	0.011	0.043	0.014	0.038	

Robust standard errors in parentheses. \* p<0.10, \*\* p<0.05, \*\*\* p<0.01.

Individual characteristics are the same as in the previous tables (see table 17A in appendix A for coefficients and significance level of the individual characteristics).

### 3.2. Social Action

We now analyze the social action. Participants had to vote to assign a £100 donation between two charities. In the first experiment we found that, overall, 49% of the participants voted in favor of donating the £100 to EFF (Electronic Frontier Foundation) rather than to TI (Transparency International), with no significant differences across treatments (pairwise chi2 tests: Positive–Negative: p-value=0.924; Negative–Neutral: p-value=0.911; Positive–Neutral: p-value= 0.989). In the second experiment, overall, 59% of the participants voted in favor of EFF, again with no significant differences across treatments (pairwise chi2 tests: Positive–Negative: p-value=0.157; Negative–Neutral: p-value=0.838; Positive–Neutral: p-value= 0.228).<sup>21</sup> Regression analysis (Table 5), where we can control for individual characteristics as well as for familiarity with the two organizations, confirms the absence of treatment differences. Not surprisingly, we find that the likelihood of voting for EFF increases as people are more familiar with its work and decreases as people are more familiar with the work of the competing charity. The likelihood of voting for EFF is sometimes higher for younger people, for males, and for non-UK nationals (see table 18A in appendix A for more details).

Overall, what emerges is that, in our setting, providing positive or negative information about privacy does not have a significant impact on social action. Also, we find that the significant impact we found for the neutral treatment in terms of self-disclosure in the second experiment does not carry over to the social action.

**Table 5 Regressions on Social action – Charity**

	Experiment 'One'		Experiment 'Two'	
	[1]	[2]	[3]	[4]
Positive treatment	-0.001 (0.05)	0.025 (0.05)	0.067 (0.06)	0.044 (0.05)
Negative treatment	-0.005 (0.05)	0.009 (0.05)	-0.011 (0.06)	-0.003 (0.05)
Constant	0.516*** (0.04)	0.882*** (0.13)	0.563*** (0.04)	0.576*** (0.15)
Individual characteristics	No	Yes	No	Yes
Charity familiarity	No	Yes	No	Yes
N	600	600	475	472
R-sqr	0.002	0.127	0.005	0.141

Robust standard errors in parentheses. \* p<0.10, \*\* p<0.05, \*\*\* p<0.01

Dependent variable: Charity – vote to donate to EFF (Electronic Frontier Foundation) was scored as '1' and vote to donate to TI (Transparency international) was scored as '0.' In all the models we control for recruitment wave. Individual characteristics are the same as in the previous table. Charity familiarity refers to level of knowledge participants had about the charity. The two variables EFF-familiarity and TI-familiarity are discrete variables, where 1 is totally unfamiliar and 5 is extensive knowledge.

<sup>21</sup> Overall, EFF received more votes than TI and, therefore, has received the donation.



### 3.3. Privacy Concern Survey

To analyze attitudes towards privacy, we follow Chellappa and Sin (2005) and ran a factor analysis on the survey. Recall that the first six questions were designed to understand the value that participants ascribe to personalization (questions Att1-Att6), the following four questions were designed to evaluate the level of concern about online privacy (questions Att7-Att10) and the last two questions were designed to understand the likelihood of the participants disclosing their personal data to online service providers (questions Att11-Att12).

We found three factors, for both the first and the second experiments:

1. Factor 1, labeled “Personal”, includes Att1 to Att4 (Cronbach’s alpha=0.75 for first experiment, =0.79 for the second);
2. Factor 2, “Privacy-concern”, includes Att7, Att9 and Att10 (Cronbach’s alpha=0.77 for first experiment, = 0.67 for second);
3. Factor 3, “Likely-give-info”, includes Att5, Att6, Att11 and Att12 (Cronbach’s alpha=0.70 for the first experiment, = 0.74 for the second).<sup>22</sup>

For the average of each item (Att1 – Att12), the average of the three factors as defined by Chellappa and Sin (2005) and the average of our factors see table 13A in appendix A.

To evaluate the treatment effects we created dichotomous variables for the three factors. To achieve this, we first calculated the average score for the questions, scored between 1 and 7, belonging to the corresponding factor. Then, we created a dummy variable for each factor, taking the value of ‘1’ if the average score is strictly greater than 4. Thus, the variables “Personal”, “Privacy-concern” and “Likely-give-info” take the value of 1 if the participant valued personalization, revealed concerns about privacy, or displayed a high likelihood of disclosing personal information. We found no treatment differences in the attitudinal survey - neither in the first experiment<sup>23</sup> nor in the second one<sup>24</sup>. A regression analysis confirms that “Privacy-concern” and “Likely-give-info” are indeed unrelated to treatment, whether or not we control for individual characteristics and the value of personalization, as measured by “Personal” (see Table 6). Looking at individual characteristics, we find that

---

<sup>22</sup> The factors we find differ slightly from those defined by Chellappa and Sin (2005). In their case, the first factor CS1 (Per) is the average of Att1-Att6 questions; the second CS2 (Concern) is the average of Att7-Att10 questions, while the last CS3 (Likely) is the average of Att11-Att12 questions.

<sup>23</sup> Pairwise chi2 tests. Personal: Positive-Negative: p=0.976; Negative –Neutral: p=0.586; Positive-Neutral: p= 0.567; Privacy-concern: Positive-Negative: p=0.895; Negative –Neutral: p=0.298; Positive-Neutral: p= 0.242; Likely-give-info: Positive-Negative: p=0.279; Negative –Neutral: p=0.997; Positive-Neutral: p= 0.274.

<sup>24</sup> Pairwise chi2 tests. Personal: Positive-Negative: p=0.809; Negative –Neutral: p=0.597; Positive-Neutral: p= 0.446; Privacy-concern: Positive-Negative: p=0.769; Negative –Neutral: p=0.734; Positive-Neutral: p= 0.965; Likely-give-info: Positive-Negative: p=0.598; Negative –Neutral: p=0.669; Positive-Neutral: p= 0.919.

males, unemployed people and high school students tend to be more concerned about their privacy, while those who value personalization are more concerned about their privacy and are less likely to provide information (thus making personalization more difficult). See table 19A in appendix A for more detailed results.

#### **4. Conclusions**

In this paper, we explored how people respond to information about privacy, either in the form of statements from privacy policies of major online companies or from news reports. We experimentally varied whether the information to which consumers are exposed reveals a positive or negative privacy practice of the company or whether this practice is neutral vis-à-vis users. We then observed the self-disclosure of personal information by users, their stated concerns regarding privacy and their choice of giving a donation either to a charity advocating for privacy or to a charity unrelated to privacy issues. What we find is that whenever information is about privacy, the type of information (positive, neutral or negative) does not matter, while information not mentioning privacy increases disclosure of personal data, without affecting either stated privacy concerns or social actions.

These findings suggest that privacy saliency may be an important aspect in privacy decision-making. We could then expect that online users will be more careful in the type of information they choose to disclose if privacy issues are more widely discussed in the public arena, for instance because of scandals related to data leakage or thefts (e.g. the recent examples regarding the US Post Office, or financial institution JPMorgan Chase & Co, or big retailers like Target, Kmart and Home Depot). A more cautious attitude in response to data thefts news is not too surprising. Our results, however, suggest that even news about increased data protection for consumers, for instance through legislative initiatives, would trigger the same reaction. Notably, in our setting, users react through *personal* actions, but not through *social* actions. This suggests that the “voice” response to privacy issues may be relatively weak, with obvious implications for the political process.

From a business perspective, it seems that making privacy policies more visible and transparent might backfire as this could nudge users to become more reluctant to share personal information and thereby derail existing business models that are based on tracking and sharing personal information. The question of how to reconcile the need to respect users’ privacy with the need to not cause major disruption in a multi-billion dollar industry is a major challenge for policy makers, businesses and academics working in the area.

**Table 6 Regressions on Privacy concern – Survey**

	Privacy concern				Likely Give Information			
	Experiment 'One'		Experiment 'Two'		Experiment 'One'		Experiment 'Two'	
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
Positive treatment	0.058 (0.05)	0.069 (0.05)	0.001 (0.06)	0.015 (0.05)	-0.045 (0.04)	-0.052 (0.04)	-0.004 (0.04)	0.001 (0.04)
Negative treatment	0.051 (0.05)	0.048 (0.05)	0.018 (0.05)	0.032 (0.05)	-0.000 (0.04)	0.004 (0.04)	0.017 (0.04)	0.025 (0.04)
Constant	0.517*** (0.04)	0.265** (0.13)	0.629*** (0.04)	0.256* (0.14)	0.795*** (0.03)	1.040*** (0.12)	0.825*** (0.03)	0.961*** (0.09)
Individual characteristics	No	Yes	No	Yes	No	Yes	No	Yes
Personalization	No	Yes	No	Yes	No	Yes	No	Yes
N	600	600	475	472	600	600	475	472
R-sqr	0.003	0.189	0.006	0.143	0.003	0.044	0.002	0.033

Robust standard errors in parentheses

\* p<0.10, \*\* p<0.05, \*\*\* p<0.01

Binary dependent variables: Privacy concern – scored as ‘1’ if the factor concern was higher than 4; Likely give information – scored as ‘1’ if the factor likely give info was higher than 4. In all the models we control for recruitment wave. Individual characteristics are the same as in the previous tables. Personalization - scored as ‘1’ if the factor personalization was higher than 4.

## References

- Acquisti A (2004) Privacy in Electronic Commerce and the Economics of Immediate Gratification. In Proceedings of the 5<sup>th</sup> ACM Electronic Commerce Conference (pp. 21-29). New York: ACM Press.
- Acquisti A, Grossklags J (2005a) Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy* 3(1): 26-33.
- Acquisti, A., Grossklags, J. (2005b). Uncertainty, Ambiguity and Privacy. In FOURTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS05)
- Acquisti A, Grossklags J (2007). What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technologies and Practices* 18: 363-377.
- Acquisti A, Grossklags J (2012) An online survey experiment on ambiguity and privacy. *Communications & Strategies* 88: 19-39.
- Acquisti A, John L K, Loewenstein G (2013). What is privacy worth? *The Journal of Legal Studies* 42(2): 249-274.
- Acquisti A, Brandimarte L, Loewenstein G (2015a) Privacy and human behavior in the age of information. *Science* 347(6221): 509-514.
- Acquisti A, Taylor C R, Wagman L (2015b) The economics of privacy. *Journal of Economic Literature*, forthcoming.
- Adjerid I, Acquisti A, Brandimarte L, Loewenstein G (2013) Sleights of privacy: Framing, disclosures, and the limits of transparency. In Proceedings of the Ninth Symposium on Usable Privacy and Security (p. 9). ACM.
- Adjerid I, Peer E, Acquisti A (2014) Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making. Working paper.
- Benndorf V, Kübler D, Normann H-T (2015) Privacy concerns, voluntary disclosure of information, and unraveling: An experiment. *European Economic Review* 75: 43-59.
- Baddeley M (2011) Information security: Lessons from behavioural economics. In Workshop on the Economics of Information Security.
- Beresford AR, Kübler D, Preibusch S (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters* 117(1): 25-27.
- Brandimarte L, Acquisti A. (2012) The Economics of Privacy. In M Peitz, J Waldfogel J (Eds), *The Oxford Handbook of the Digital Economy*, pp. 547- 571, Oxford, UK: Oxford University Press.
- Buchanan T, Paine C, Joinson AN, Reips UD (2007) Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58(2): 157-165.
- Campbell J, Goldfarb A, Tucker C (2015) Privacy regulation and market structure. *Journal of Economics & Management Strategy* 24(1): 47-73.
- Casadesus-Masanell R, Hervás-Drane A (2015) Competing with Privacy. *Management Science* 61(1): 229-246.
- Caudill EM, Murphy PE (2000) Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing* 19(1): 7-19.
- Chellappa RK, Sin RG (2005) Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2-3): 181-202.
- Chellappa RK, Shivendu S (2010) Mechanism design for “free” but “no free disposal” services: The economics of personalization under privacy concerns. *Management Science* 56(10): 1766-1780.
- Culnan MJ (1993) ‘How Did They Get My Name’? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly* 17(3): 341-364.
- Culnan MJ, Armstrong PK (1999) Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science* 10(1): 104-115.
- Dinev T, Hart P (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research* 17(1): 61-80.
- Goldfarb A, Tucker CE (2011) Privacy regulation and online advertising. *Management Science* 57(1): 57-71.
- Goldfarb A, Tucker CE (2012) Shifts in Privacy Concerns. *American Economic Review* 102(3): 349-53.
- Hann I-H, Hui K-L, Lee SYT, Png IPL (2008) Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems* 24(2):13-42.
- Hirschman AO (1970) *Exit, Voice and Loyalty*. Harvard University Press, Cambridge/Massachusetts.
- Howe N, Strauss W (2000) *Millennials Rising - The Next Great Generation*. Vintage.
- Hui K, Png I (2006) Economics of Privacy. In T Hendershott (Ed.). *Handbook of Information Systems and Economics*, pp. 471-497, Elsevier.
- Jensen C, Potts C (2004) Privacy policies as decision-making tools: an evaluation of online privacy notices. Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pp. 471-478.
- Jensen C, Potts C (2005) Privacy Practices of Internet Users: Self-reports versus Observed Behavior. *International Journal of Human-Computer Studies* 63: 203- 227.
- John LK, Acquisti A, Loewenstein G (2011) Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, 37(5): 858-873.

- Joinson AN, Paine C, Buchanan T, Reips UD (2008) Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior*, 24(5): 2158-2171.
- McDonald A, Cranor L (2008) The Cost of Reading Privacy Policies. Telecommunications Policy Research Conference.
- Malhotra NK, Kim SS, Agarwal J (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15(4): 336-355.
- Malheiros M, Preibusch S, Sasse MA (2013) "Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. In *Trust and Trustworthy Computing* (pp. 250-266). Springer Berlin Heidelberg.
- Marreiros H, Gomer R, Vlassopoulos M, Tonin M, Schraefel M (2015) Scared or Naïve? An Exploratory study of user perceptions of online privacy disclosures. *IADIS International Journal of WWW/Internet* 13(2): 1-16.
- Milne GR, Rohm A (2000) Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives. *Journal of Public Policy and Marketing* 19(2): 238-249.
- Norberg PA, Horne DR, Horne DA (2007) The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal of Consumer Affairs* 41(1): 100-126.
- Olivero N, Lunt P (2004) Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2): 243-262.
- Phelps J, Nowak G, Ferrell E (2000) Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy and Marketing* 19(1): 27-41.
- Posner RA (1981) The Economics of Privacy. *American Economic Review* 71(2): 405-409.
- Privacy Leadership Initiative. (2001). Privacy Notices Research Final Results. Conducted by Harris Interactive, December 2001.
- Shy, O, Stenbacka R (2015) Customer privacy and competition. *Journal of Economics & Management Strategy*. doi: 10.1111/jems.12157
- Stigler GJ (1980) An Introduction to Privacy in Economics and Politics. *Journal of Legal Studies* 9: 623-644.
- TRUSTe (2006), "TRUSTe make your privacy choice", available at: [www.truste.org/](http://www.truste.org/)
- Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* 22(2): 254-268.
- Turow J, Feldman L, Meltzer K (2005) Open to Exploitation: American Shoppers Online and Offline. The Annenberg Public Policy Center.
- Varian HR (1997) Economic Aspects of Personal Privacy. Privacy and Self-Regulation in the Information Age, National Telecommunications and Information Administration, US Department of Commerce.
- Vila T, Greenstadt R, Molnar D (2003) Why we can't be bothered to read privacy policies: privacy as a lemons market. In Fifth International Conference on Electronic Commerce, ICEC.
- Xu H, Teo HH, Tan BCY, Agarwal R (2010) The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems* 26(3): 137-176.

**Appendix A: Tables – Experiments ‘One’ and ‘Two’**

Table 1A: Characterization of the subject pool - Experiment ‘One’

	<b>All</b>		<b>Positive treatment</b>		<b>Negative treatment</b>		<b>Neutral treatment</b>		Min	Max
	N	%	N	%	N	%	N	%		
Age	600	28*	194	28	198	29*	208	28*	18	67
Age - millennial	600	77%	194	75%	198	76%	208	79%	0	1
Sex	600	52%	194	53%	198	48%	208	56%	0	1
UK national	600	69%	194	69%	198	71%	208	68%	0	1
US national	600	24%	194	23%	198	23%	208	24%	0	1
White	600	85%	194	85%	198	87%	208	84%	0	1
Student status	579	58%	183	57%	191	58%	205	58%	0	1
Full time	600	42%	194	42%	198	42%	208	42%	0	1
Part time	600	22%	194	24%	198	20%	208	23%	0	1
Unemployed	600	18%	194	16%	198	20%	208	18%	0	1
High school	600	15%	194	12%	198	18%	208	15%	0	1
College	600	71%	194	74%	198	68%	208	69%	0	1
Post-grad	600	13%	194	12%	198	13%	208	14%	0	1
Income [Less 20000] **	600	50%	194	55%	198	44%	208	49%	0	1
Income [20000-40000] **	600	26%	194	23%	198	32%	208	23%	0	1
Income [40000-60000] **	600	9%	194	7%	198	9%	208	12%	0	1
Income [More 60000] **	600	4%	194	4%	198	3%	208	5%	0	1
Time taken (min)	600	9*	194	8*	198	9*	208	9*	4	46.4

Age and time taken are continuous variables; all the other variables are binary. \*Average. \*\*Annual income.

Table 2A: Characterization of the subject pool - Experiment 'Two'

	All		Positive treatment		Negative treatment		Neutral treatment		Min	Max
	N	%	N	%	N	%	N	%		
Age	475	28*	154	29*	163	28*	158	28*	18	67
Age - millennial	475	80%	154	79%	163	80%	158	81%	0	1
Sex	475	47%	154	42%	163	47%	158	52%	0	1
UK national	475	27%	154	28%	163	25%	158	28%	0	1
US national	475	63%	154	64%	163	61%	158	64%	0	1
White	475	81%	154	85%	163	75%	158	82%	0	1
Student status	468	45%	151	48%	160	45%	157	43%	0	1
Full time	475	38%	154	37%	163	40%	158	36%	0	1
Part time	475	31%	154	25%	163	29%	158	38%	0	1
Unemployed	475	20%	154	23%	163	17%	158	20%	0	1
High school	475	15%	154	11%	163	16%	158	19%	0	1
College	475	73%	154	77%	163	72%	158	69%	0	1
Post-grad	475	12%	154	12%	163	12%	158	12%	0	1
Income [Less 20000] **	475	39%	154	36%	163	39%	158	41%	0	1
Income [20000-40000] **	475	31%	154	33%	163	31%	158	28%	0	1
Income [40000-60000] **	475	14%	154	11%	163	15%	158	15%	0	1
Income [More 60000] **	475	9%	154	8%	163	7%	158	10%	0	1
Time taken (min)	475	13*	154	12*	163	13*	158	13*	5	55

Age and time taken are continuous variables; all the other variables are binary. \*Average. \*\*Annual income.

Table 3A: Participants' classification of privacy policy statements and news extracts

Used in the Positive Treatments						
	<i>Privacy Policy Statement</i>			<i>Dropbox News</i>		
	<b>Positive</b>	Negative	Neutral	<b>Positive</b>	Negative	Neutral
Positive Treatment	81%	2%	17%	86%	3%	10%
Negative Treatment	86%	3%	11%	82%	3%	15%
Neutral Treatment	88%	1%	12%	84%	1%	15%
<b>Total</b>	<b>85%</b>	<b>2%</b>	<b>13%</b>	<b>84%</b>	<b>2%</b>	<b>14%</b>

Used in the Negative Treatments						
	<i>Privacy Policy Statement</i>			<i>Facebook News</i>		
	Positive	<b>Negative</b>	Neutral	Positive	<b>Negative</b>	Neutral
Positive Treatment	4%	76%	20%	4%	94%	2%
Negative Treatment	2%	78%	20%	0%	91%	9%
Neutral Treatment	1%	77%	22%	1%	92%	7%
<b>Total</b>	<b>2%</b>	<b>77%</b>	<b>21%</b>	<b>1%</b>	<b>92%</b>	<b>6%</b>

Used in the Neutral Treatments						
	<i>Privacy Policy Statement</i>			<i>Wearable News</i>		
	Positive	Negative	<b>Neutral</b>	Positive	Negative	<b>Neutral</b>
Positive Treatment	10%	17%	73%	27%	14%	60%
Negative Treatment	8%	17%	75%	22%	16%	62%
Neutral Treatment	5%	25%	71%	31%	15%	54%
<b>Total</b>	<b>7%</b>	<b>20%</b>	<b>73%</b>	<b>27%</b>	<b>15%</b>	<b>59%</b>

Rows 1 to 7 refer to the positive treatments, rows 8 to 14 refer to the negative treatments and rows 15 to 21 refer to the neutral treatments.

The 1<sup>st</sup> column refers to each treatment. The 2<sup>nd</sup> column indicates the percentage of participants that classified as positive the privacy policy statement used in experiment 'one' and the 5<sup>th</sup> column indicates the percentage of those who classified as positive the news extracts used in experiment 'two' in each treatment. The 3<sup>rd</sup> and 6<sup>th</sup> columns indicate the percentage of participants that classified it as negative, and the 4<sup>th</sup> and 7<sup>th</sup> columns indicate the percentage of participants that classified it as neutral.



Table 4A - Demographics - Experiment 'one'

	All		Positive treatment		Negative treatment		Neutral treatment	
	N	% "Prefer not to say"	N	% "Prefer not to say"	N	% "Prefer not to say"	N	% "Prefer not to say"
Age	600	0.3%	194	0.5%	198	0.5%	208	0.0%
Health	600	1.2%	194	0.5%	198	1.0%	208	1.9%
Marital Status	600	1.2%	194	2.1%	198	1.5%	208	0.0%
Education	600	1.3%	194	1.5%	198	1.0%	208	1.4%
Moved house	600	1.8%	194	2.1%	198	2.0%	208	1.4%
Gender	600	0.7%	194	0.5%	198	0.5%	208	1.0%
No. Children	600	1.0%	194	1.0%	198	1.0%	208	1.0%
No. Credit cards	600	3.3%	194	2.1%	198	4.5%	208	3.4%
Debt situation	600	4.3%	194	3.6%	198	5.1%	208	4.3%
Country live	600	0.0%	194	0.0%	198	0.0%	208	0.0%
Relationship length	600	9.8%	194	12.4%	198	7.1%	208	10.1%
Annual income	600	11.2%	194	11.3%	198	11.1%	208	11.1%
Spend week	600	7.8%	194	6.7%	198	9.6%	208	7.2%

Use of the option "prefer not to say" is scored as "1" and disclosure of the information is scored as "0".

Table 5A - Charity - experiment 'one'

	All		Positive treatment		Negative treatment		Neutral treatment	
	N	% Eff votes	N	% Eff votes	N	% Eff votes	N	% Eff votes
Charity	600	48.8%	194	49.0%	198	48.5%	208	49.0%

Votes to donate to EFF are scored as "1" and votes to donate to T.I. are scored as "0".

Table 6A- Demographics - Experiment 'two'

	<b>All</b>		<b>Positive treatment</b>		<b>Negative treatment</b>		<b>Neutral treatment</b>	
	N	%	N	%	N	%	N	%
Age	475	0.0%	154	0.0%	163	0.0%	158	0.0%
Health	475	0.4%	154	0.0%	163	0.0%	158	1.3%
Marital Status	475	0.6%	154	0.6%	163	0.6%	158	0.6%
Education	475	0.2%	154	0.6%	163	0.0%	158	0.0%
Moved house	475	0.4%	154	1.3%	163	0.0%	158	0.0%
Gender	475	0.2%	154	0.0%	163	0.0%	158	0.6%
No. Children	475	0.4%	154	0.0%	163	0.6%	158	0.6%
No. Credit cards	475	1.5%	154	1.3%	163	1.2%	158	1.9%
Debt situation	475	2.1%	154	3.2%	163	1.2%	158	1.9%
Country live in	475	0.0%	154	0.0%	163	0.0%	158	0.0%
Relationship	475	7.6%	154	9.1%	163	7.4%	158	6.3%
Annual income	475	8.4%	154	11.7%	163	7.4%	158	6.3%
Spend week	475	5.7%	154	5.8%	163	4.3%	158	7.0%

Use of the option “prefer not to say” is scored as “1” and disclose the information is scored as “0”.

Table 7A - Charity - Experiment 'two'

	<b>All</b>		<b>Positive treatment</b>		<b>Negative treatment</b>		<b>Neutral treatment</b>	
	N	% Eff votes	N	% Eff votes	N	% Eff votes	N	% Eff votes
Charity	475	58.7%	154	63.6%	163	55.8%	158	57.0%

Votes to donate to EFF are scored as “1” and votes to donate to T.I. are scored as “0”.

Table 8A: Percentage of match between the demographic information collected from Prolific Academic and the information that participants disclosed.

	Positive	Negative	Neutral	Total
<i>Experiment 1</i>				
Age	94%	92%	97%	95%
Gender	100%	99%	100%	100%
Country	96%	96%	98%	97%
<i>Experiment 2</i>				
Age	98%	98%	97%	97%
Gender	100%	99%	99%	99%
Country	92%	87%	89%	89%

Table 9A: Knowledge of the presence of the statements in the privacy policy and about the companies' practices reported in the news extracts.

	Positive	Negative	Neutral	Total
Awareness of Privacy Policy	46%	33%	39%	40%
Awareness of Practices - News	14%	47%	77%	46%
Total	32%	40%	55%	42%

Table 10A: Perception of friends' knowledge of the presence of the statement in the privacy policy and about the companies' practices reported in the news extracts.

	Positive	Negative	Neutral	Total
Awareness of Privacy Policy	24%	0%	18%	14%
Awareness of Practices - News	7%	25%	66%	33%
Total	17%	11%	39%	22%

Table 11A: Perception of society's knowledge of presence of the statement in the privacy policy and about the companies' practices reported in the news extracts.

	Positive	Negative	Neutral	Total
Awareness of Privacy Policy	19%	11%	13%	14%
Awareness of Practices - News	7%	11%	47%	21%
Total	13%	27%	11%	17%

Table 12A: Sensitive questions

	All		Positive treatment		Negative treatment		Neutral treatment	
	N	% "PNS"	N	% "PNS"	N	% "PNS"	N	% "PNS"
Religious	475	4%	154	5%	163	4%	158	4%
Race	475	2%	154	3%	163	1%	158	3%
No sexual partners	475	19%	154	22%	163	18%	158	18%
No serious relations	475	11%	154	10%	163	13%	158	10%
Partner's gender	475	10%	154	9%	163	12%	158	9%
Weight	475	32%	154	37%	163	34%	158	24%
High school name	475	65%	154	71%	163	67%	158	58%
Passport number	475	100%	154	100%	163	100%	158	100%
Name first pet	475	60%	154	62%	163	66%	158	51%
Mother maiden name	475	86%	154	84%	163	90%	158	85%
Favorite place	475	46%	154	51%	163	50%	158	39%

%PNS: Percentage of participants using the option "Prefer not to say."

Table 13A: Attitudes

	Experiment 'One'				Experiment 'Two'			
	All	Positive	Negative	Neutral	All	Positive	Negative	Neutral
Att1	5.54	5.45	5.52	5.63	5.46	5.50	5.40	5.48
Att2	4.91	4.95	4.87	4.91	5.00	4.97	4.88	5.13
Att3	4.03	4.16	3.86	4.06	3.92	3.90	3.75	4.11
Att4	3.97	3.99	3.99	3.94	3.95	3.79	3.86	4.21
Att5	4.59	4.45	4.69	4.64	4.58	4.55	4.59	4.61
Att6	5.68	5.58	5.65	5.79	5.82	5.90	5.91	5.65
Att7	3.99	4.10	3.86	3.99	4.08	3.99	4.07	4.18
Att8	5.99	6.02	5.96	5.99	5.96	5.92	5.96	6.00
Att9	3.76	3.85	3.82	3.62	3.88	3.88	3.87	3.90
Att10	4.85	4.78	4.82	4.93	5.04	5.08	4.98	5.05
Att11	4.76	4.64	4.84	4.79	4.97	4.97	4.85	5.08
Att12	5.10	5.11	5.17	5.02	5.27	5.29	5.18	5.34
CS1 (Per)	4.78	4.76	4.76	4.83	4.79	4.77	4.73	4.87
CS2 (Concern)	4.64	4.69	4.62	4.63	4.74	4.71	4.72	4.78
CS3 (Likely)	4.93	4.88	5.00	4.91	5.12	5.13	5.01	5.21
Personal (Av)	4.61	4.64	4.56	4.64	4.58	4.54	4.47	4.73
Privacy concern (Av)	4.20	4.24	4.17	4.18	4.33	4.31	4.31	4.38
Likely give info (Av)	5.03	4.95	5.09	5.06	5.16	5.18	5.13	5.17

Likert 7-point scale: Strongly disagree=1 to Strongly agree=7. [Att1-Att6] indicates the average of value for personalization; [Att7-Att10] indicates the average of privacy concerns and [Att11 and Att12] indicates the average of the likelihood of disclosing information.

Chellappa and Sin Factors: CS1(Per): Average [Att1-Att6]; CS2 (Concern): Average [Att7-Att10]; CS3 (Likely): Average [Att11-Att12];

Data Factors: Personal (Av): Average [Att1-Att4]; Privacy concern (Av): Average [Att7, Att9-Att10]; Likely give info (Av): Average [Att5-Att6, Att10-Att11].

Table 14A: Regressions on self-disclosure - Experiment 'one'

	Disclosure- Index	Give Name	Give Email
	[1]	[2]	[3]
Positive treatment	0.025 (0.03)	-0.027 (0.05)	-0.044 (0.05)
Negative treatment	0.043 (0.03)	0.009 (0.05)	0.004 (0.05)
Wave	0.006 (0.03)	-0.170*** (0.04)	-0.157*** (0.04)
Age	-0.002 (0.00)	-0.004* (0.00)	-0.002 (0.00)
Gender	-0.048 (0.03)	-0.020 (0.04)	-0.049 (0.04)
UK nationality	-0.037 (0.06)	0.122 (0.08)	0.038 (0.07)
US nationality	-0.012 (0.06)	0.238*** (0.08)	0.093 (0.08)
White	0.115*** (0.04)	0.221*** (0.06)	0.088* (0.05)
Student	-0.030 (0.03)	-0.094* (0.05)	-0.039 (0.05)
College	0.026 (0.04)	0.020 (0.06)	0.052 (0.05)
Post-grad	-0.015 (0.06)	-0.079 (0.08)	0.038 (0.07)
Full time	-0.001 (0.04)	0.055 (0.06)	0.080 (0.06)
Part time	-0.016 (0.04)	0.084 (0.07)	0.097 (0.06)
Unemployed	0.023 (0.04)	0.036 (0.07)	0.122* (0.06)
Income [Less -20000]	0.691*** (0.05)	0.130** (0.06)	0.165*** (0.05)
Income [20000-40000]	0.645*** (0.05)	0.133** (0.06)	0.208*** (0.06)
Income [40000-60000]	0.757*** (0.05)	0.166** (0.08)	0.251*** (0.08)
Constant	0.062 (0.10)	0.242 (0.15)	0.117 (0.15)
N	579	579	579
R-sqr	0.383	0.096	0.077

Robust standard errors in parentheses. \*p&lt;0.10, \*\* p&lt;0.05, \*\*\* p&lt;0.001

Table 15A: Regressions on self-disclosure – Experiment ‘two’

	Disclosure-Index	Give Name	Give Email
	[1]	[2]	[3]
Positive treatment	0.001 (0.04)	-0.156*** (0.06)	-0.140** (0.06)
Negative treatment	0.053 (0.03)	-0.111** (0.06)	-0.132** (0.06)
Wave	-0.025 (0.03)	-0.141*** (0.05)	-0.064 (0.05)
Age	0.001 (0.00)	0.006** (0.00)	0.002 (0.00)
Gender	-0.024 (0.03)	-0.029 (0.05)	0.006 (0.05)
UK nationality	-0.063 (0.05)	0.018 (0.09)	-0.001 (0.09)
US nationality	-0.017 (0.04)	-0.082 (0.08)	-0.064 (0.08)
White	0.138*** (0.04)	0.050 (0.06)	-0.034 (0.06)
Student	-0.010 (0.03)	0.019 (0.06)	-0.055 (0.05)
College	0.137*** (0.05)	-0.077 (0.06)	-0.168** (0.07)
Post-grad	0.163** (0.07)	-0.169* (0.09)	-0.201** (0.09)
Full time	0.243*** (0.07)	0.051 (0.08)	0.052 (0.08)
Part-time	0.196*** (0.06)	0.001 (0.08)	0.011 (0.08)
Unemployed	0.153** (0.07)	0.181** (0.09)	0.107 (0.08)
Income [Less -20000]	0.383*** (0.06)	0.073 (0.07)	0.067 (0.07)
Income [20000-40000]	0.386*** (0.06)	0.205*** (0.07)	0.113 (0.07)
Income [40000-60000]	0.349*** (0.06)	0.016 (0.09)	0.051 (0.08)
Constant	0.114 (0.10)	0.434*** (0.15)	0.566*** (0.15)
N	465	465	465
R-sqr	0.291	0.092	0.062

Robust standard errors in parentheses. \*p<0.10, \*\* p<0.05, \*\*\* p<0.001

Table 16A: Sensitive questions

	Disclosure_index_SQ	
	[1]	[2]
Positive	-0.529** (0.24)	-0.502** (0.25)
Negative	-0.534** (0.23)	-0.455* (0.23)
Wave	-0.206 (0.19)	-0.212 (0.20)
Age		0.012 (0.01)
Gender		-0.307 (0.20)
UK nationality		-0.136 (0.37)
US nationality		-0.127 (0.30)
White		0.577** (0.26)
Student		0.490** (0.24)
College		0.933** (0.38)
Postgrad		1.105*** (0.39)
Full-time		-0.316 (0.28)
Part-time		-0.880** (0.41)
Unemployed		0.694* (0.39)
Income [Less20000]		0.208 (0.29)
Income [20000-40000]		0.445 (0.31)
Income [40000-60000]		0.210 (0.38)
Constant	8.089*** (0.20)	6.609*** (0.67)
N	475	465
R-sqr	0.016	0.085

Robust standard errors in parentheses. \*p<0.10, \*\* p<0.05, \*\*\* p<0.001



Table 17A- Experiment Differences in Disclosure of information

	Index Demo	Give Name	Give Email
	[1]	[2]	[3]
Positive Exp 'One'	-0.032 (0.04)	-0.136** (0.06)	-0.158*** (0.05)
Positive Exp 'Two'	-0.000 (0.04)	-0.133** (0.06)	-0.141** (0.06)
Negative Exp 'One'	-0.011 (0.04)	-0.116** (0.06)	-0.119** (0.05)
Negative Exp 'Two'	0.044 (0.04)	-0.099* (0.06)	-0.130** (0.05)
Neutral Exp 'One'	-0.056 (0.04)	-0.113** (0.06)	-0.119** (0.05)
Age	0.001 (0.00)	0.000 (0.00)	-0.000 (0.00)
Gender	-0.042** (0.02)	-0.031 (0.03)	-0.034 (0.03)
UK nationality	-0.029 (0.04)	0.019 (0.06)	-0.020 (0.06)
US nationality	0.004 (0.04)	0.028 (0.06)	-0.021 (0.06)
White	0.127*** (0.03)	0.125*** (0.04)	0.017 (0.04)
Student	-0.025 (0.02)	-0.044 (0.04)	-0.056 (0.04)
College	0.071** (0.03)	-0.037 (0.04)	-0.053 (0.04)
Post-grad	0.064 (0.04)	-0.140** (0.06)	-0.074 (0.06)
Full-time	0.080** (0.04)	0.026 (0.05)	0.050 (0.05)
Part-time	0.063* (0.04)	0.033 (0.05)	0.050 (0.05)
Unemployed	0.051 (0.04)	0.066 (0.05)	0.097* (0.05)
Income [Less20000]	0.553*** (0.04)	0.112** (0.05)	0.123*** (0.04)
Income [20000-40000]	0.533*** (0.04)	0.168*** (0.05)	0.164*** (0.04)
Income [40000-60000]	0.573*** (0.04)	0.105* (0.06)	0.161*** (0.06)
Constant	0.140* (0.07)	0.387*** (0.11)	0.385*** (0.11)
N	1044	1044	1044
R-sqr	0.318	0.043	0.038

Robust standard errors in parentheses. \*p<0.10, \*\* p<0.05, \*\*\* p<0.001

Table 18A: Regressions on Social action – charity

	Experiment 'One'	Experiment 'Two'
	[1]	[2]
Positive	0.025 (0.05)	0.044 (0.05)
Negative	0.009 (0.05)	-0.003 (0.05)
Wave	-0.052 (0.04)	0.001 (0.05)
Age	-0.004* (0.00)	-0.003 (0.00)
Gender	-0.061 (0.04)	-0.087* (0.05)
UK nationality	-0.135* (0.08)	-0.019 (0.08)
US nationality	-0.023 (0.08)	0.002 (0.07)
White	-0.000 (0.06)	-0.034 (0.06)
College	0.023 (0.06)	0.061 (0.06)
Postgrad	0.043 (0.07)	0.054 (0.09)
Full-time	0.025 (0.06)	0.140* (0.08)
Part-time	0.045 (0.06)	0.069 (0.08)
Unemployed	0.027 (0.06)	0.080 (0.08)
Income [Less20000]	-0.082 (0.06)	0.073 (0.07)
Income [20000-40000]	-0.109* (0.06)	-0.055 (0.07)
Income [40000-60000]	-0.178** (0.08)	-0.020 (0.08)
EFF familiarity	0.169*** (0.03)	0.198*** (0.03)
TI familiarity	-0.275*** (0.03)	-0.224*** (0.04)
Constant	0.882*** (0.13)	0.576*** (0.15)
N	600	472
R-sqr	0.127	0.141

Robust standard errors in parentheses. \*p<0.10, \*\* p<0.05, \*\*\* p<0.001

Table 19A: Regressions on Privacy concern – Survey

	Privacy concern		Likely Give Information	
	Experiment 'One'	Experiment 'Two'	Experiment 'One'	Experiment 'Two'
	[1]	[2]	[3]	[4]
Positive	0.069 (0.05)	0.015 (0.05)	-0.052 (0.04)	0.001 (0.04)
Negative	0.048 (0.05)	0.032 (0.05)	0.004 (0.04)	0.025 (0.04)
Wave	-0.024 (0.04)	-0.070 (0.04)	0.016 (0.03)	0.028 (0.03)
Age	-0.003 (0.00)	0.002 (0.00)	-0.002 (0.00)	0.002 (0.00)
Gender	-0.096** (0.04)	-0.101** (0.04)	0.003 (0.03)	0.046 (0.04)
UK nationality	0.095 (0.08)	0.071 (0.08)	-0.023 (0.07)	-0.085 (0.06)
US nationality	0.088 (0.08)	0.068 (0.08)	-0.012 (0.07)	-0.031 (0.06)
White	-0.035 (0.05)	0.044 (0.06)	-0.125*** (0.04)	0.022 (0.05)
College	-0.114** (0.05)	-0.095 (0.06)	0.038 (0.05)	-0.061 (0.04)
Postgrad	-0.149** (0.07)	-0.238*** (0.09)	0.052 (0.06)	-0.019 (0.06)
Full-time	0.094* (0.06)	0.094 (0.08)	0.003 (0.05)	-0.032 (0.06)
Part-time	0.094 (0.06)	0.052 (0.08)	-0.080 (0.05)	-0.010 (0.06)
Unemployed	0.133** (0.06)	0.071 (0.08)	-0.052 (0.06)	-0.043 (0.06)
Income [Less20000]	0.109* (0.06)	0.078 (0.07)	0.015 (0.05)	-0.082* (0.04)
Income [20000-40000]	0.111* (0.06)	0.093 (0.07)	-0.018 (0.06)	-0.123*** (0.05)
Income [40000-60000]	0.078 (0.08)	0.191** (0.09)	-0.083 (0.07)	-0.115* (0.06)
Personalization	0.387*** (0.04)	0.304*** (0.05)	-0.114*** (0.03)	-0.039 (0.04)
Constant	0.265** (0.13)	0.256* (0.14)	1.040*** (0.12)	0.961*** (0.09)
N	600	472	600	472
R-sqr	0.189	0.143	0.044	0.033

Robust standard errors in parentheses. \*p&lt;0.10, \*\* p&lt;0.05, \*\*\* p&lt;0.001

## Appendix B

### 1. Privacy policy statements:

**Positive treatment:** Collected from Google privacy policy.

*“We do not share personal information with companies, organizations and individuals outside of Google unless we have your consent.”*

**Negative treatment:** Collected from Facebook data policy.

*“We share information we have about you within the family of companies that are part of Facebook.”*

**Neutral treatment:** Collected from Facebook data policy.

*“Cookies are small pieces of data that are stored on your computer, mobile phone or other device. Pixels are small blocks of code on webpages that do things like allow another server to measure viewing of a webpage and often are used in connection with cookies.”*

### 2. Extract of newspaper articles:

**Positive treatment:** Collected from *computerweekly.com* on the 18th May 2015.

#### **"Dropbox secures data privacy-focused ISO 27018 standard"**

"Dropbox has followed in the footsteps of Microsoft to become an early adopter of the privacy-focused ISO 27018 standard, which is used to signify how providers safeguard users' cloud data.

The standard sets out a code of practice that governs how users' personally identifiable information should be protected by cloud providers.

Organisations that adhere to the ISO 27018 code of practice, therefore, must vow not to use this information in sales and marketing materials, and must promise to provide users with details about where their data is kept and handled and to notify them straightaway in the event of a data breach."

**Negative treatment:** Collected from *sherbit.io* on the 17th April 2015.

### **"How Facebook Inc (FB) Is Getting Rich Using Your Personal Data"**

"Researchers with the Belgian Privacy Commission conducted a comprehensive analysis of Facebook's new Data Use Policy and Terms of Service and concluded that the company is in violation of European law: it has authorized itself to continuously collect users' location information, sell users' photos for advertising purposes, and track both users' and non-users' browsing habits across the internet—while failing to educate users on the true extent of this 'tracking,' and making it prohibitively difficult for them to 'opt-out.'

Facebook's cookies are stored in every browser that visits a site with a Social Plugin (the embedded 'Like' and 'Share' buttons), regardless of whether or not they are a Facebook user. "

**Neutral treatment:** Collected from *computing.co.uk* on the 12th February 2015.

### **"Why Wearable Tech Is Good for Your Health"**

"The Apple Watch and Adidas's plans for including wearable technology in its shoe and clothing lines have been drawing attention recently, as the age of always-accessible information is upon us.

In the era of the Internet of Things — when our homes are linked to our smartphones and everything else is linked to a network — it's still somewhat surprising to realize that entire industries have yet to be transformed by increased connectivity. Until recently, one of those areas was arguably the health field.

Yes, files have been switched to online servers for some time now. But it's only been in the past year or so that the health industry has begun to be revolutionized by the possibilities technology offers."