Title: "Now that you mention it": A Survey Experiment on Information, Inattention and Online Privacy

Authors: Helia Marreiros, Mirco Tonin, Michael Vlassopoulos, M.C. Schraefel

PII: S0167-2681(17)30089-6
DOI: http://dx.doi.org/doi:10.1016/j.jebo.2017.03.024
Reference: JEBO 4018

To appear in: *Journal of Economic Behavior & Organization*

Received date: 29-11-2016
Revised date: 21-3-2017
Accepted date: 30-3-2017

Please cite this article as: Marreiros, Helia, Tonin, Mirco, Vlassopoulos, Michael, Schraefel, M.C., "Now that you mention it": A Survey Experiment on Information, Inattention and Online Privacy.Journal of Economic Behavior and Organization http://dx.doi.org/10.1016/j.jebo.2017.03.024

"Now that you mention it": A Survey Experiment on Information, Inattention and Online Privacy

Helia Marreiros[a], Mirco Tonin[b,*], Michael Vlassopoulos[c], m.c. schraefel[d].

[a] University of Southampton, Economics Department, School of Social Sciences, SO17 1BJ Southampton, UK. helia.r.marreiros@gmail.com

[a] University of Southampton, Economics Department, School of Social Sciences, SO17 1BJ Southampton, UK. m.vlassopoulos@soton.ac.uk

[b] Free University of Bolzano, Faculty of Economics and Management, 39100, Bolzano, Italy; IZA, Bonn; CESifo, Munich; Dondena, Milan. Mirco.Tonin@unibz.it

[c] University of Southampton, Electronics and Computer Sciences Department, SO17 1BJ Southampton, UK.

Highlights

- We investigate whether information affects consumers' privacy actions and attitudes
- We explore how people react to information regarding privacy reported in the news
- Participants disclose less identifiable information when exposed to information
- Even when information relates to positive features of privacy
- Privacy concerns are dormant and manifest when users are asked to think about privacy

Abstract

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 may have incomplete information or may be inattentive about the digital transactions of their data. This paper investigates whether highlighting positive or negative aspects of online privacy policies, thereby mitigating the informational problem, can affect consumers' privacy actions and attitudes. Results of an online survey experiment indicate that participants adopt a more conservative stance on disclosing sensitive and identifiable information, even when positive attitudes of companies towards their privacy are made salient, compared to when privacy is not mentioned. On the other hand, they do not change their attitudes and social actions towards privacy. These findings suggest that privacy behavior is not necessarily sensitive to exposure to objective threats or benefits of disclosing personal information. Rather, people are inattentive and their dormant privacy concerns may manifest only when consumers are asked to think about privacy.

JEL classification: C83, L38, M38

Keywords: survey experiment; information economics; privacy; inattention; self-disclosure; consumer behavior

*Corresponding author. Email address: mirco.tonin@unibz.it

Abstract

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 may have incomplete information or may be inattentive about the digital transactions of their data. This paper investigates whether highlighting positive or negative aspects of online privacy policies, thereby mitigating the informational problem, can affect consumers' privacy actions and attitudes. Results of an online survey experiment indicate that participants adopt a more conservative stance on disclosing sensitive and identifiable information, even when positive attitudes of companies towards their privacy are made salient, compared to when privacy is not mentioned. On the other hand, they do not change their attitudes and social actions towards privacy. These findings suggest that privacy behavior is not necessarily sensitive to exposure to objective threats or benefits of disclosing personal information. Rather, people are inattentive and their dormant privacy concerns may manifest only when consumers are asked to think about privacy.

JEL classification: C83, L38, M38

Keywords: survey experiment; information economics; privacy; inattention; salience; self-disclosure; consumer behavior

1. Introduction

Agreeing with the terms and conditions and privacy policies of online service providers has become an almost daily task for billions of people worldwide.[1] 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, Facebook and Amazon (Taylor 2004, Casadesus-Masanell and Hervas-Drane 2015). Despite giving formal consent, consumers are often unaware of

[1] As of March 31, 2016, Facebook had 1.65 billion monthly active users. http://newsroom.fb.com/company-info/

what these digital transactions involve (Acquisti et al. 2015b) 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,[2] 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. For instance, reforming data protection rules in the EU is currently a policy priority for the European Commission.[3] 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).[4]

The standard approach to privacy posits that consumers use all available information to make privacy decisions considering the benefits and costs associated with revealing personal information (e.g. Acquisti et al. 2015b, Posner 1981, Stigler 1980, Varian 1997). In other words, 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, Hui and Png 2006, 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

[2] 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/).

[3] 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. The General Data Protection Regulation (GDPR) will be a law in the beginning of 2018. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[4] 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).

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).[5]

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). Furthermore, there is growing evidence emerging from psychology and behavioral economics that bounded rationality and several behavioral biases and heuristics influence individuals' decision-making in this realm. Examples are optimism bias (e.g. Baek et al. 2014), overconfidence (Jensen et al. 2005, Brandimarte et al. 2013) and hyperbolic discounting (Acquisti and Grossklags 2003, 2005a). Consequently, individuals face incomplete information, bounded rationality and behavioral biases, which can affect their choices regarding sharing personal information online (Acquisti 2004, Acquisti and Grossklags 2005a, 2007, Baddeley 2011, Reidenberg et al. 2015).

In this paper, we experimentally investigate to what extent exposure to information about how online companies deal with personal information (trading or not personal data) influences privacy decisions. In particular, we investigate whether information about the degree of privacy protection has an impact on disclosure actions and on privacy attitudes, as well as on social actions. Becoming more aware of the threats

[5] The three main benefits of the privacy trade-off 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) and social interactions and network externalities (Lin and Lu 2011). See also Acquisti (2015b) for an overview of the cost and benefits of sharing information for both data holders and data subjects.

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

As privacy-related stories attract more headlines in mainstream media,[6] an interesting question is to explore how people react to information regarding privacy reported in the news. Thus, we investigate whether news coverage of actual privacy practices by companies affects users' privacy preferences. To address this question, we conducted an online survey experiment, with around 500 respondents, involving an informational intervention. In particular, 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.[7]

Our experimental design involves three treatments. Participants are randomly presented with a newspaper article extract highlighting a positive, neutral or negative privacy practice. 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.

[6] 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 a study where Londoners accepted the terms and conditions for access to public Wi-Fi with a clause stating that they accept to give up their eldest children in exchange for Wi-Fi. Most of the participants accepted the clause, however, obviously, did not have to give up their child (http://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause).

[7] The information used in the experiment was rated in a pre-test as reflecting either a positive, negative or neutral attitude towards their users, by students of the University of Southampton.

This design allows us to examine two alternative hypotheses. First, 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 experiment, highlighting positive (negative) features of the privacy tradeoff (such as protection of consumers' personal data vs commercial exploitation of their data) 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 is social action promoting privacy protection. Another possible driver of behavior in this study relates to the recent literature in economics that shows that limited attention, salience and cognitive costs impact decision making in a variety of contexts: consumption (Chetty et al., 2009; Hossain and Morgan, 2006; Bollinger et al., 2011; Allcott and Taubinsky, 2015), saving (Karlan et al., 2016), farming (Hanna et al., 2014) or school choice (Hastings and Weinstein, 2008). Two of our informational treatments (positive and negative), contain news articles related to privacy, which might focus participants' attention to the issue of privacy - independent of the actual information that the news item conveys about businesses' privacy practices. Differently to what the first hypothesis predicts, if participants are inattentive to privacy at the beginning of the survey, they might reduce their willingness to disclose personal information upon prompted to focus on the issue in both the positive and negative treatments.

We find that the propensity of participants to disclose identifiable information (such as name, email) and sensitive information (such as mother's middle name) decreases when they are exposed to information regarding privacy. 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 how 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. In this regard, the paper connects to recent research that proposes that individuals may only attend to information that they consider relevant for the decision at hand and that interventions that help decision makers attend to key neglected dimensions may improve outcomes (Schwartzstein, 2014; Hanna et al., 2014; LaRiviere and

Neilson, 2015). Our result is also consistent with previous findings that contextual cues (Benndorf et al. 2015, John et al. 2011, Hughes-Roberts and Kani-Zabihi, 2014) and notifications about privacy breaches (Feri et al. 2016) do have an impact on levels of disclosure of sensitive information and, more generally, with the literature on salience and framing effects (Stasser 1992, Druckman 2001, Levin et al. 1998, Kahneman 2003).

Despite finding an effect on disclosure we do not find treatment effects on social actions, nor on privacy attitudes. In the privacy literature, this disconnect between actions and attitudes - 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 states the hypotheses, while section 4 presents the results. Section 5 offers some conclusions. Appendix A contains some additional results.

2. Experimental Design and Sample

To understand the effect of highlighting positive and negative privacy practices on the behavior of online users, we designed an online survey experiment. We recruited a total of 508 participants in June 2015 (in two waves), using Prolific Academic, a UK-based crowdsourcing community that recruits participants for academic purposes.[8] Each participant received the amount of £1 upon completion of a survey that took on average 10 minutes to complete, which translated as £6 per hour, on average. The recruitment was restricted to participants born in the UK, the US, Ireland, Australia and Canada, and whose first language was English. The experiment was designed in Qualtrics Online Sample, and the randomization of treatments was programmed in the survey software.[9]

[8] Prolific Academic is a crowdsourcing platform for scientific studies in which researchers post studies and recruit participants. It is used by academic researchers worldwide and has a worldwide participant pool with more than 50,000 reliable participants. More information about the platform is available at www.prolific.ac. A recent comparison across online platforms (including M-Turk and Prolific Academic) by Peer et al. (2016) reveals that participants in Prolific Academic are less dishonest and more naïve, in the meaning that they display less familiarity with commonly used research materials, compared to M-Turk and produced data quality comparable to M-Turk's.

[9] The survey is available as supplementary material.

2.1. Experimental Manipulations

As experimental manipulations, we used extracts from newspaper articles.[10] These news extracts provided information that highlighted a positive, a negative or a neutral aspect of companies' privacy practices and were selected through a pre-test, where we asked 25 students to evaluate the news extracts.

In particular, 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 not directly related to privacy issues.

We use a between-subject design, where each participant is exposed to only one treatment - i.e. is exposed to only one of the extracts - before we measure privacy preferences. To further validate our experimental manipulation, at the end we asked participants to classify the three extracts 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

To start with, 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 1998, and that The University of Southampton ethics committee had approved the study.[11] 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 a foundation unrelated to privacy;

[10] A transcription of the news extracts can be found in appendix B.
[11] More information is available at http://www.southampton.ac.uk/legalservices/what-we-do/data-protection-and-foi.page

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.[12] 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. Providing name and email was optional, as a scroll-down option was not possible. 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 5A in appendix A for detailed information). Moreover, most names matched the emails, when provided. 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.[13]

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 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

[12] 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).

[13] 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."

issues) or Transparency International (an organization that fights against corruption and is therefore not directly related 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.[14,15]

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.

Finally, participants were asked to reply to eleven sensitive questions structured in the same way as the initial questionnaire. For instance, we asked information on the number and gender 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. Sensitive questions might have a higher impact on participants' willingness to disclose information (Joison 2008).

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 news extracts used in the experiment revealed a positive, negative or neutral attitude of the company towards their users. Second, we asked if participants were more or less willing to share their personal data online after reading these extracts and if they were willing to pay a small fee to protect their identifiable and non-identifiable information. Third, we added a final survey about online privacy concerns (Buchanan et al. 2007); our decision to include this was

[14] "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

[15] "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

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 experiment, e.g. whether participants usually read privacy policies or already knew of the two non-profit organizations.

2.3. Characterization of the Subject Pool

Our final sample consists of 475 participants.[16] 47% of the participants were female and the average age was 28, with 80% part of the "millennial generation" (i.e. born between 1982 and 2004: Howe and Strauss 2000). Most of the participants were from the US, 63%, or the UK, 27%; 81% were white and 45% were students; 73% had two to four years of college education; and 70% had an income lower than 40.000 (in local currency) [17]. The average time to complete the survey was thirteen minutes (see table 1A in appendix A for more detailed descriptive statistics). These characteristics are balanced across the three treatments.

3. Hypotheses

Our experimental design allows us to investigate the extent to which participants are using the informational content of the news messages to inform the privacy decisions in the experiment or whether instead the messages serve to focus their attention to the fact that there is a privacy context in the decision-making.

Previous evidence suggests that perceived privacy risks raise privacy concerns and have an adverse effect on willingness to reveal personal information (Dinev and Hart 2006, Malhotra et al. 2004). If the messages have informational value, we then expect participants in the negative treatment to be less willing to share information in the first stage, less likely to support the charity promoting digital rights in the second stage and to display more conservative attitudes toward privacy and personalization in stage 3, than participants in the neutral and

[16] Out of the initial 508 participants, we rejected 33 submissions in total: 8 submissions from those that fail the control question (which asked to skip that question) and 25 submissions from those that completed the survey in less than 5 minutes. The aim is to exclude those who did not take the task seriously, not reading the questions or doing it extremely quickly. We find similar results running the analysis with the full sample.

[17] Information about gender, nationality, education, student and employment status was provided by Prolific Academic. Information about income level was provided by the participants in the self-disclosure stage. Prolific Academic only had information about student status for 465 participants.

positive treatments. Similarly, we expect participants in the positive treatment to be more relaxed about sharing private information than those in the neutral treatment.

> **Hypothesis 1:** (Information) People's privacy attitudes and actions will respond to the informational content of the message they see.

Another possibility is that participants are not unaware of the information regarding privacy that we transmit to them. However, the mere mention of privacy in the messages might make them more attentive to the issue. This perspective would be consistent with existing theoretical work and evidence that when decision makers have limited attention, inefficient decisions can be made not due to lack of information, but due to failure to attend to some features of the data (Hanna et al., 2014; LaRiviere and Neilson, 2015).

> **Hypothesis 2:** (Inattention) People's privacy attitudes and actions will not respond to the actual information content of the message they see, but their privacy attitudes and actions will be affected when prompted to think about privacy.

Accordingly, we expect participants to be more conservative in treatments negative and positive than in the neutral treatment, as the latter does not focus attention on privacy.

4. 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 news extracts used in that experiment as representing a positive, negative or neutral attitude of the company towards its users. What we found is that 84% of the participants considered that the extract chosen for the positive treatment indeed reflected a positive attitude; 93% of the participants classified the extract chosen for the negative treatment as negative; and 59% of the participants

classified the extract chosen for the neutral treatment as neutral[18] (see table 2A in appendix A for more details). Thus, the majority of the participants classified correctly the news extract after being presented with it.

4.1. Self-disclosure

To analyze treatment effects, 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 that can take values between 0 (if no information is provided) and 13 (if information is provided for all 13 demographic questions). We then created three variables measuring self-disclosure, all taking the values 0/1:

1. Disclosure: equals 1 if the participant discloses personal information in all the first 13 items of the demographic questionnaire;[19]
2. Give Name: equals 1 if the participant discloses their first name;
3. Give Email: equals 1 if the participant discloses their email address.

Table 1 describes the percentages of disclosure of information per treatment. We can observe that the large majority of participants (84%) disclosed all the personal information that could not directly identify them as individuals.[20] 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 50% provided their first name) and email (only 37% disclosed their email address). With the exception of three participants, those who disclosed email also disclosed name. 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. However, we did not find significant differences between the positive and

[18] In the neutral treatment 27% classified the extract as positive and 14% as negative.
[19] 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.
[20] See table 3A 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.

the negative treatments;[21] thus it does not seem to be the case that providing "negative" information makes participants more reluctant to disclose private information.

These results are confirmed in a regression analysis (Table 2), 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.[22,23] Also, including a dummy controlling for previous awareness of the information we provide gives similar results (for summary statistics of awareness see tables 6A to 8A in appendix A).[24]

As mentioned in the previous section, participants were also asked to disclose 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 9A for non-disclosure percentages per variable and per treatment).

[21]Chi2 test: Positive – Negative: Disclosure: p-value=0.146; Give-name: 0.664; Give-email: 0.709; Negative-Neutral: Disclosure: p-value=0.291; Give-name: 0.028; Give-email: 0.012; Neutral – Positive: Disclosure: p-value=0.688; Give-name: 0.009; Give-email: 0.005.

[22] Our results indicate that less wealthy individuals and white people are more likely to disclose personal information (for details, see table 11A in appendix A). The results on the relationship between wealth and self-disclosure are consistent with those of Goldfarb and Tucker (2012). The income variables are divided in five dummy variables - Annual_income_less_20; Annual_income_20_40; Annual_income_40_60; Annual_income_more_60 and Prefer_not_reveal_income. The variable prefer not to reveal income was the omitted variable.

[23] Given that, as shown in table 2A, 31% of the participants of the neutral treatment considered the statement positive, as a robustness check, we run the OLS regressions excluding them. Even in this case, participants disclose significantly less information in the positive treatment. The coefficients when controlling for individual characteristics are 0.027 (s.e. 0.04) for the Disclosure-Index, -0.139** (s.e. 0.06) for Give Name and -0.126** (s.e. 0.06) for Give Email.

[24] We present the results of OLS regression analysis, as they are easy to interpret. Logit and Probit models give similar results. Poisson and Tobit regressions for the Disclosure-index also give similar results.

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[25]. 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 Poisson regression analysis, with and without controls for individual characteristics (see table 12A in appendix A).

What is the interpretation of these results? Participants do not seem to react in the way predicted in Hypothesis 1 (Information), with positive information inducing more disclosure and negative information increasing their concern for privacy. The fact that participants disclosed more information in the neutral treatment, where privacy was not mentioned, as the information provided referred to the advantages of wearable tech, than in the other treatments suggests that, consistently with Hypothesis 2 (Inattention), being prompted to think privacy issues has an effect on individual online behavior, decreasing self-disclosure.

As in Joinson et al. (2008), just mentioning privacy focuses 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.

4.2. Social Action

[25] 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.

We now analyze the social action. Participants had to vote to assign a £100 donation between two charities. We found that, overall, 59% of the participants voted in favor of EFF, 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).[26,27] Regression analysis (Table 3), 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 (see table 13A in appendix A for more details). Thus, it seems that the significant impact we found for the neutral treatment in terms of self-disclosure does not carry over to the social action.

4.3. 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:

1. Factor 1, labeled "Personal", includes Att1 to Att4 (Cronbach's alpha=0.79);
2. Factor 2, "Privacy-concern", includes Att7, Att9 and Att10 (Cronbach's alpha=0.67);
3. Factor 3, "Likely-give-info", includes Att5, Att6, Att11 and Att12 (Cronbach's alpha=0.74).[28]

[26] Overall, EFF received more votes than TI and, therefore, has received the donation.

[27] See table 4A in Appendix A for treatment differences.

[28] 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. In our factor analysis Att8 is not part of any of the three factors. In a Varimax rotation at 0.4 Att8 is eliminated, therefore factor 2 'privacy-concern' is constituted by attributes Att7, Att9 and Att10. Att8 refers to concerns about anonymous information collected

For the average of each item (Att1 – Att12), and the average of the factors see table 10A 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[29]. 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 "Personalization" (see Table 4). Looking at individual characteristics, we find that 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 13A in appendix A for more detailed results.

5. Conclusions

In this paper, we explored how people respond to information about privacy in the form of 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 information is neutral vis-à-vis users' privacy. 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 not directly related to privacy issues. What we find is that whenever information is about privacy, the type of information (positive or negative) does

automatically that cannot be used to identify the users, such as computer, network information and operating system. The results are similar including att8.

[29] 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.

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 inattention 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 practices 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 the right of users to make informed choices about online privacy with the current business model of a multibillion-dollar industry is a major challenge for policy makers, businesses and academics working in the area.

ACKNOWLEDGMENTS

We acknowledge financial support from Research Councils UK via the Meaningful Consent in the Digital Economy Project - grant reference EP/K039989/1.

References

Acquisti A (2004) Privacy in Electronic Commerce and the Economics of Immediate Gratification. In Proceedings of the *5th ACM Electronic Commerce Conference* (pp. 21-29). New York: ACM Press.

Acquisti A, Grossklags J. (2003). Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior. In: Proceedings of the *2nd annual workshop on economics and information security (WEIS 2003)*, May 29–30, Maryland, USA

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, 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, 5:2*, 442-492.

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.

Allcott, H., and Taubinsky, D. (2015) Evaluating behaviorally motivated policy: experimental evidence from the lightbulb market. *American Economic Review*, *105*(8), 2501-2538.

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior, 31*, 48-56.

Baddeley M (2011) Information security: Lessons from behavioural economics. In *Workshop on the Economics of Information Security*.

Benndorf V, Kübler D, Normann H-T (2015) Privacy concerns, voluntary disclosure of information, and unraveling: An experiment. *European Economic Review 75*, 43-59.

Beresford AR, Kübler D, Preibusch S (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters 117(1)*, 25-27.

Bollinger, B., Leslie, P., Sorensen, A. (2011). Calorie posting in chain restaurants. *American Economic Journal: Economic Policy*, *3*(1), 91-128.

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.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science, 4(3),* 340-347.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (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, Hervas-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.

Chetty, R, A Looney, Kroft K (2009) Salience and taxation: Theory and evidence. *American Economic Review,* 99(4): 1145-1177.

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.

Druckman, J. N. (2001). Evaluating framing effects. *Journal of Economic Psychology, 22(1),* 91-101.

Feri, F., Giannetti, C., & Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior & Organization, 123*, 138-148.

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.

Hanna, R., Mullainathan, S., Schwartzstein, J. (2014). Learning through noticing: Theory and evidence from a field experiment. *The Quarterly Journal of Economics*, *129*(3), 1311-1353.

Hastings, J. S., Weinstein, J. M. (2008). Information, school choice, and academic achievement: Evidence from two experiments. *The Quarterly journal of economics*, *123*(4), 1373-1414.

Hirschman AO (1970) Exit, Voice and Loyalty. *Harvard University Press*, Cambridge/Massachussets.

Hossain T, J Morgan (2006) ...Plus Shipping and Handling: Revenue (Non)Equivalence in Field Experiments on eBay. *Advances in Economic Analysis and Policy*, Vol. 6.

Howe N, Strauss W (2000) Millennials Rising - The Next Great Generation. Vintage.

Hughes-Roberts, T., Kani-Zabihi, E. (2014). On-Line Privacy Behavior: Using User Interfaces for Salient Factors. *Journal of Computer and Communications, 2(04)*, 220.

Hui K, Png I (2006) Economics of Privacy. In T Hendershott (Ed.). *Handbook of Information Systems and Economics,* 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*, 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.

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. *The American economic review, 93(5),* 1449-1475.

Karlan, D., McConnell, M., Mullainathan, S., and Zinman, J. (2016). Getting to the top of mind: How reminders increase saving. *Management Science*, *62*(12), 3393-3411.

Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: A typology and critical analysis of framing effects. *Organizational behavior and human decision processes, 76(2),* 149-188.

Lin, K. Y., & Lu, H. P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior, 27(3),* 1152-1161.

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.

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.

Peer, E, Sonam S, Brandimarte, L and Acquisti, A (2016) Beyond the Turk: An Empirical Comparison of Alternative Platforms for Crowdsourcing Online Behavioral Research. Available at SSRN: https://ssrn.com/abstract=2594183 or http://dx.doi.org/10.2139/ssrn.2594183

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.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., & Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Tech. LJ,* 30, 39.

Stasser, G. (1992). Information salience and the discovery of hidden profiles by decision-making groups: A "thought experiment". *Organizational Behavior and Human Decision Processes, 52(1),* 156-181.

Shy, O, Stenbacka R (2015) Customer privacy and competition. *Journal of Economics & Management Strategy.*

Stigler GJ (1980) An Introduction to Privacy in Economics and Politics. *Journal of Legal Studies 9*, 623–644.

Schwartzstein, J. (2014). Selective attention and learning. *Journal of the European Economic Association*, *12*(6), 1423-1452.

TRUSTe (2006), "TRUSTe make your privacy choice", available at: www.truste.org/

Taylor, C. R. (2004). Consumer privacy and the market for customer information. *RAND Journal of Economics,* 631-650.

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.

Web references:

http://newsroom.fb.com/company-info/ Last accessed 14th July, 2016

http://ec.europa.eu/justice/data-protection/reform/index_en.htm. Last accessed 14th July, 2016

http://consumersunion.org/news/poll-consumers-concerned-about-internet-privacy/ September 25, 2008. Last accessed 14th July, 2016

http://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause. Last accessed 14th July, 2016

https://www.eff.org. Last accessed 14th July, 2016

http://www.transparency.org. Last accessed 14th July, 2016

Table 1 Self-disclosure stage

	All		**Positive treatment**		*Pos - Neg*	**Negative treatment**		*Neg - Neu*	**Neutral treatment**		*Neu – Pc*
	N	% "DIS"	N	% "DIS"	p-value	N	% "DIS"	p-value	N	% "DIS"	p-value
Disclosure	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

	Disclosure		Give Name		Give Email	
	[1]	[2]	[3]	[4]	[5]	[6]
Positive treatment	-0.018	0.026	-0.148***	-0.152***	-0.157***	-0.134**
	(0.04)	(0.03)	(0.06)	(0.06)	(0.05)	(0.06)
Negative treatment	0.042	0.057	-0.123**	-0.111**	-0.137**	-0.132**
	(0.04)	(0.03)	(0.06)	(0.06)	(0.05)	(0.06)
Constant	0.833***	-0.153**	0.637***	0.401***	0.482***	0.507***
	(0.04)	(0.07)	(0.04)	(0.15)	(0.04)	(0.15)
Individual characteristics	No	Yes	No	Yes	No	Yes
N	475	465	475	465	475	465
R-sqr	0.005	0.499	0.025	0.094	0.022	0.068

Robust standard errors in parentheses.

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

Dependent variables: Disclosure - 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 non-UK) ethnicity (white or not) Student and work status, education and income (see table 11A in appendix A for coefficients and significance level of the individual characteristics).

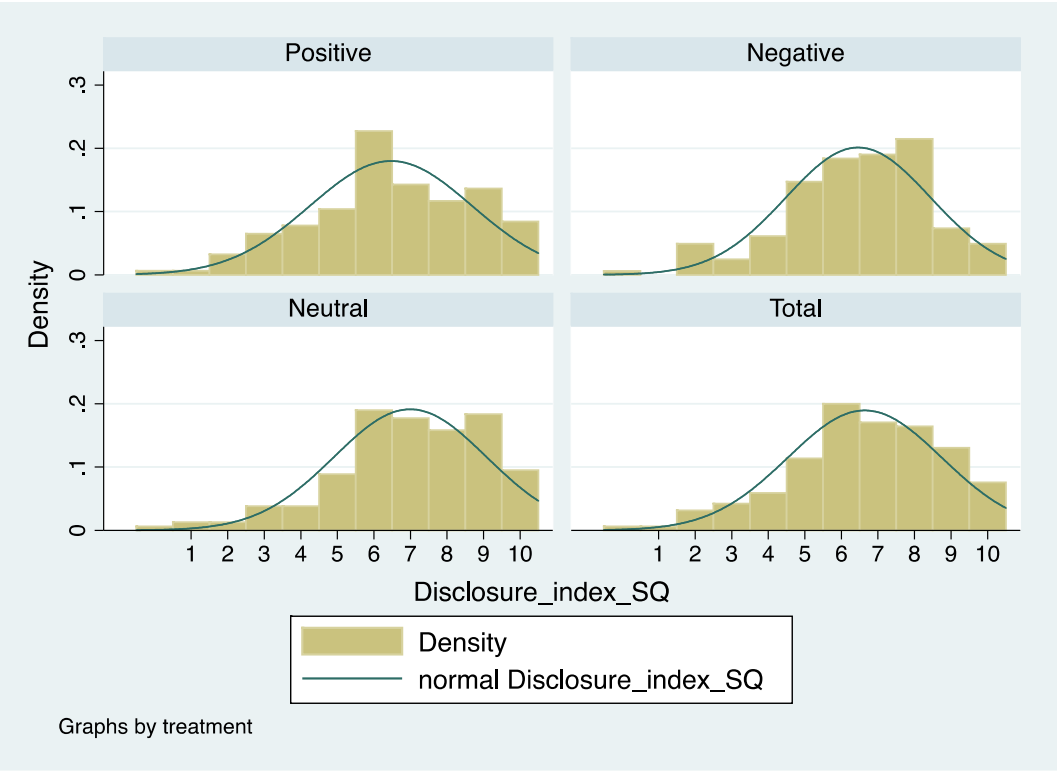

Figure 1 Histogram of the disclosure of sensitive items

Table 3 Regressions on Social action – Charity

	[1]	[2]
Positive treatment	0.067	0.055
	(0.06)	(0.05)
Negative treatment	-0.011	0.004
	(0.06)	(0.05)
Constant	0.563***	0.738***
	(0.04)	(0.16)
Individual characteristics	No	Yes
Charity familiarity	No	Yes
N	475	465
R-sqr	0.005	0.147

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.

Table 4 Regressions on Privacy concern – Survey

	Privacy concern		Likely Give Information	
	[1]	[2]	[3]	[4]
Positive treatment	0.001	0.002	-0.004	-0.000
	(0.06)	(0.06)	(0.04)	(0.04)
Negative treatment	0.018	0.027	0.017	0.025

	(0.05)	(0.05)	(0.04)	(0.04)
Constant	0.629***	0.258	0.825***	0.954***
	(0.04)	(0.16)	(0.03)	(0.10)
Individual characteristics	No	Yes	No	Yes
Personalization	No	Yes	No	Yes
N	475	465	475	465
R-sqr	0.006	0.145	0.002	0.032

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.

Appendix A: Tables

Table 1A: Characterization of the subject pool

	All		Positive treatment		Negative treatment		Neutral treatment			
	N	%	N	%	N	%	N	%	Min	Max
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.

The characterization of the subject pool is based on demographics provided by prolific academic, with the exception of Income, which is based on the information the participants provided during the experiment in the stage of self-disclosure.

Table 2A: Participants' classification of news extracts

A. Used in the Positive Treatments: Dropbox News

	Positive	Negative	Neutral
Positive Treatment	87%	3%	10%
Negative Treatment	82%	3%	15%
Neutral Treatment	84%	1%	15%
Total	84%	2%	14%

B. Used in the Negative Treatments: Facebook News

	Positive	**Negative**	Neutral
Positive Treatment	4%	94%	2%
Negative Treatment	0%	91%	9%
Neutral Treatment	1%	92%	7%
Total	1%	93%	6%

C. Used in the Neutral Treatments: Wearable News

	Positive	Negative	**Neutral**
Positive Treatment	27%	14%	60%
Negative Treatment	22%	16%	62%
Neutral Treatment	31%	15%	54%
Total	27%	14%	59%

Panel A refers to the news extracts used in the positive treatments, Panel B refers to the news extracts used in the negative treatments and Panel C refers to the news extracts used in the neutral treatments. The 1st column of each panel refers to the treatments. The 2nd column of each panel indicates the percentage of participants that classified the news extracts as positive, in each treatment. Therefore, in the Panel A, the percentage presented in the 2nd column (Positive), 2nd row (Positive treatment) indicates how many participants in the positive treatment classified the extract as positive. The percentage presented in the 2nd column (Positive), 3rd row (Negative treatment) indicates how many participants in the negative treatment classified the extract as positive. The percentage presented in the 3nd column (Negative), 2nd row (Positive treatment) indicates how many participants in the positive treatment classified the extract as negative. And so forth. The 3rd column indicate the percentage of participants that classified the extracts as negative, and the 4th column indicate the percentage of participants that classified it as neutral.

Table 3A- Demographics

	All		**Positive treatment**		**Negative treatment**		**Neutral treatment**	
	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 4A - Charity

	All		Positive treatment		Negative treatment		Neutral treatment	
	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 5A: Percentage of match between the demographic information collected from Prolific Academic and the information that participants disclosed.

	Positive	Negative	Neutral	Total
Age	98%	98%	97%	97%
Gender	100%	99%	99%	99%
Country	92%	87%	89%	89%

Table 6A: Knowledge about the companies' practices reported in the news extracts.

	Positive	Negative	Neutral	Total
Awareness of Practices	14%	47%	77%	46%

Table 7A: Perception of friends' knowledge about the companies' practices reported in the news extracts.

	Positive	Negative	Neutral	Total
Awareness of Practices	7%	25%	66%	33%

Table 8A: Perception of society's knowledge about the companies' practices reported in the news extracts.

	Positive	Negative	Neutral	Total
Awareness of Practices	7%	11%	47%	21%

Table 9A: 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 10A: Attitudes

	All	Positive	Negative	Neutral
Att1	5.46	5.50	5.40	5.48
Att2	5.00	4.97	4.88	5.13
Att3	3.92	3.90	3.75	4.11
Att4	3.95	3.79	3.86	4.21
Att5	4.58	4.55	4.59	4.61
Att6	5.82	5.90	5.91	5.65
Att7	4.08	3.99	4.07	4.18
Att8	5.96	5.92	5.96	6.00

Att9	3.88	3.88	3.87	3.90
Att10	5.04	5.08	4.98	5.05
Att11	4.97	4.97	4.85	5.08
Att12	5.27	5.29	5.18	5.34
Personal (Av)	4.58	4.54	4.47	4.73
Privacy concern (Av)	4.33	4.31	4.31	4.38
Likely give info (Av)	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.

Factors: Personal (Av): Average [Att1-Att4]; Privacy concern (Av): Average [Att7, Att9-Att10]; Likely give info (Av): Average [Att5-Att6, Att10-Att11]. Att8 was excluded in the factor analysis, as it does not belong to any of the 3 factors and is excluded from the varimax rotation at 0.4 Including att8 leads to the same results.

Table 11A: Regressions on self-disclosure

	Disclosure	Give Name	Give Email
	[1]	[2]	[3]
Positive treatment	0.026	-0.152***	-0.134**
	(0.03)	(0.06)	(0.06)
Negative treatment	0.057*	-0.111**	-0.132**
	(0.03)	(0.06)	(0.06)
Wave	-0.027	-0.141***	-0.064
	(0.03)	(0.05)	(0.05)
Age	0.001	0.006**	0.002
	(0.00)	(0.00)	(0.00)
Gender	0.004	-0.026	0.012
	(0.02)	(0.05)	(0.05)
US nationality	-0.071**	-0.088	-0.076
	(0.03)	(0.08)	(0.08)
White	0.071*	0.042	-0.049
	(0.04)	(0.06)	(0.06)
Student	0.015	0.022	-0.050
	(0.03)	(0.06)	(0.05)
College	0.090**	-0.083	-0.178***
	(0.04)	(0.06)	(0.07)
Post-grad	0.018	-0.187**	-0.234**
	(0.06)	(0.09)	(0.09)
Full time	0.134**	0.038	0.028
	(0.06)	(0.09)	(0.08)
Part-time	0.106*	-0.009	-0.009
	(0.06)	(0.08)	(0.08)
Unemployed	0.100*	0.175**	0.096
	(0.06)	(0.09)	(0.08)

Income [<20000]	0.836***	0.127	0.168*
	(0.04)	(0.09)	(0.09)
Income [20000-40000]	0.864***	0.262***	0.219**
	(0.04)	(0.09)	(0.09)
Income [40000-60000]	0.844***	0.076	0.161
	(0.05)	(0.11)	(0.10)
Income [>60000]	0.901***	0.109	0.200*
	(0.05)	(0.11)	(0.11)
Constant	-0.153**	0.401***	0.507***
	(0.07)	(0.15)	(0.15)
N	465	465	465
R-sqr	0.499	0.094	0.068

Robust standard errors in parentheses. *p<0.10, ** p<0.05, *** p<0.001. Individual characteristics, with the exception of income, come from Prolific Academic and are provided by users when registering. To control for income, we use responses to our own demographic questionnaire, with people not revealing their income as the omitted category.

Table 12A: Sensitive questions – Poisson regression

	Disclosure_index_SQ	
	[1]	[2]
Positive treatment	-0.068**	-0.061*
	(0.03)	(0.03)
Negative treatment	-0.069**	-0.058**
	(0.03)	(0.03)
Wave	-0.027	-0.029
	(0.03)	(0.03)
Age		0.002
		(0.00)
Gender		-0.036

		(0.03)
US nationality		-0.024
		(0.04)
White		0.067*
		(0.04)
Student		0.069**
		(0.03)
College		-0.048
		(0.03)
Postgrad		-0.142***
		(0.05)
Full-time		0.081
		(0.06)
Part-time		0.115**
		(0.05)
Unemployed		0.144***
		(0.05)
Income [<20000]		0.106*
		(0.06)
Income [20000-40000]		0.141**
		(0.06)
Income [40000-60000]		0.114*
		(0.06)
Income [>60000]		0.150**
		(0.07)
Constant	2.091***	1.835***
	(0.02)	(0.09)
N	475	465
Pseudo R-sqr	0.002	0.012

Actual coefficients are reported. Robust standard errors in parentheses. *p<0.10, ** p<0.05, *** p<0.001. See footnote to Table 11A.

Table 13A: Regressions on Social action and Attitudes

	Charity	Privacy concern	Likely Give Information
Positive	0.055	0.002	-0.000
	(0.05)	(0.06)	(0.04)
Negative	0.004	0.027	0.025
	(0.05)	(0.05)	(0.04)
Wave	-0.001	-0.068	0.027
	(0.05)	(0.04)	(0.04)
Age	-0.006**	0.002	0.002
	(0.00)	(0.00)	(0.00)
Gender	-0.100**	-0.095**	0.045
	(0.05)	(0.05)	(0.04)
US nationality	-0.006	0.069	-0.030
	(0.07)	(0.08)	(0.06)
White	-0.040	0.052	0.027
	(0.06)	(0.06)	(0.05)
Student	-0.104**	0.021	-0.001
	(0.05)	(0.05)	(0.04)
College	0.078	-0.087	-0.058
	(0.06)	(0.06)	(0.04)
Postgrad	0.074	-0.221**	-0.015
	(0.09)	(0.09)	(0.06)
Full-time	0.090	0.070	-0.029
	(0.08)	(0.08)	(0.06)
Part-time	0.044	0.026	-0.004
	(0.08)	(0.08)	(0.06)
Unemployed	0.043	0.060	-0.038
	(0.08)	(0.08)	(0.07)
Income [<20000]	0.041	0.048	-0.089
	(0.09)	(0.09)	(0.06)

Income [20000-40000]	-0.085	0.073	-0.129**
	(0.09)	(0.09)	(0.06)
Income [40000-60000]	-0.039	0.164	-0.121
	(0.10)	(0.11)	(0.08)
Income [>60000]	-0.024	-0.038	-0.013
	(0.12)	(0.12)	(0.08)
EFF familiarity	0.196***		
	(0.03)		
TI familiarity	-0.214***		
	(0.04)		
Personalization		0.314***	-0.038
		(0.05)	(0.04)
Constant	0.738***	0.258	0.954***
	(0.16)	(0.16)	(0.10)
N	465	465	465
R-sqr	0.147	0.145	0.032

Robust standard errors in parentheses. *p<0.10, ** p<0.05, *** p<0.001. See footnote to Table 11A.

Appendix B

1. 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 there 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 c*omputing.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."