European Commission

JRC SCIENCE AND POLICY REPORT

Nudges to Privacy Behaviour: Exploring an Alternative Approach to Privacy Notices

Shara Monteleone, René van Bavel,
Nuria Rodríguez-Priego, Gabriele Esposito

2015

Report EUR 27384 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for Prospective Technological Studies

Contact information
Address: Edificio Expo. c/ Inca Garcilaso, 3. E-41092 Seville (Spain)
E-mail: jrc-ipts-secretariat@ec.europa.eu
Tel.: +34 954488318
Fax: +34 954488300

https://ec.europa.eu/jrc
https://ec.europa.eu/jrc/en/institutes/ipts

JRC96695

EUR 27384 EN

ISBN 978-92-79-50320-7 (PDF)

ISSN 1831-9424 (online)

doi:10.2791/142795

Luxembourg: Publications Office of the European Union, 2015

Abstract

The report seeks to bring behavioural research methods for privacy to the attention of EU policy-makers. It argues that changes in web interface design can be a useful policy alternative to the traditional 'privacy notice' approach. Specifically, it examines whether web interface design has effect on people's online privacy behaviour through an online experiment (n=3229) in four European countries. Results show that the presence of an anthropomorphic character leads to greater disclosure of personal information, both directly and passively and the presence of a privacy notice leads to greater direct information disclosure. Additional psychological constructs (such as subjects' awareness that they were revealing personal information) were also recorded, and a demographic analysis according to gender, age, education and country of residence carried out.

Acknowledgments

The authors are indebted to Alessandro Acquisti for advice and for leading the project *Behavioural Response to Privacy Visceral Notices* (contract no. 153752-2013-A08-IT), which collected the data; to Norberto Andrade for launching this project and guiding it through its early stages; to Ryan Calo for generous advice; to Aaron Martin for a thorough and constructive review; to Nestor Duch-Brown for comments on the statistical analysis; and to Ioannis Maghiros for continued support.

Table of Contents

Executive Summary

This report is a contribution to the discussion on how best to ensure citizens' on-line privacy while giving them the freedom to benefit as much as possible from the Internet. It explores whether changes in the design of web interfaces (i.e. the *choice architecture* according to the behavioural economics literature) lead to changes in privacy behaviour, and so merit attention as an additional policy tool. It builds on two premises: (a) the predominant model of informing users through 'privacy notices' is ineffective, as people seldom read them and (b) *nudges*, which are changes in the choice architecture to elicit a certain behaviour, have been shown to be effective in other domains.

An on-line experiment (n=3,229) across four European countries examined the effect on privacy behaviour of seven nudges. These appeared as changes in the design of a mock search engine's user interface (e.g. including an anthropomorphic character, highlighting prior browsing history or changing the look-and-feel to convey greater informality). These nudges were tested and considered relevant in previous studies (particularly Groom and Calo, 2011). Two types of privacy behaviour were measured: *passive disclosure*, when people unwittingly disclose personal information, and *direct disclosure,* when people make an active choice to reveal personal information.

In addition to directly observing privacy behaviour, the on-line experiment also included a questionnaire which sought to capture a series of psychological constructs, such as participants' perception that the experiment was trying to get them to reveal personal information inadvertently or their feelings of being observed / monitored. It also tested whether participants noticed the privacy policy link.

Selected results

- Anthropomorphic images increase subjects' predisposition to disclose personal information, either wittingly or unwittingly. This could be due to users 'letting their guard down' following an increase in trust due to the presence of an anthropomorphic character (Bente, Dratsch, Rehbach, Reyl and Lushaj, 2014).
- Actively disclosing personal information appears to be a strong cultural trait, but revealing it inadvertently less so. For direct disclosure of personal information, there were significant differences between countries; but for passive disclosure only Italy stood out from the rest (participants there revealed the most personal information inadvertently).
- Subjects with a higher level of education felt significantly less observed or monitored than those with a lower level of education, challenging the assumption that education generates greater awareness of privacy risks. However, better-educated participants did reveal less personal information inadvertently than less educated ones (no difference in direct disclosure of information).
- Approximately 73% of women answered 'never' to the stigmatized questions, compared to 27% of males. This large difference could be due to the nature of the questions (e.g. about alcohol consumption, which might be more acceptable for males). It could also suggest women feel under greater social scrutiny or simply are more cautious when disclosing personal information.

By showing the effect of nudges and demographic variables on privacy behaviour, this study highlights the value of a behavioural economics approach to data protection regulation. Further tests, either in laboratory or on-line experiments, or directly in the field (for example, when rolling out a new government website), should seek to confirm the effect of these changes and test additional ones.

The implications for policy are that, while nudges are unlikely to solve all the challenges which online privacy regulation faces, they do contribute to a solution. Good, conscientious and evidence-based website design can lead to more aware and cautious disclosure of personal data. Privacy enforcement authorities – at national or EU level – can work together with major web service providers (such as Google or Facebook), who have vast amounts of such data at their disposal, towards developing a series of 'safe practices in web design'. It is an opportunity to work together to achieve innovative and mutually-beneficial solutions to privacy challenges in the online environment.

I. Introduction

The context in which any decision is taken is referred to as the *choice architecture* in the recent nomenclature of behavioural economics. A change in this choice architecture which is intended to encourage certain behaviour is considered a *nudge*, and is distinct from a direct instruction or demand (Thaler and Sunstein, 2008). Nudges have been shown to influence behaviour across a range of policy areas, including on-line privacy behaviour (Acquisti, 2009; Acquisti, Brandimarte and Loewenstein, 2015).

Existing legal safeguards (such as privacy notices that inform users of how their personal data can be used) are supposed to foster a privacy-protective behaviour among Internet users. However, while they fulfil legal requirements, they have been relatively ineffective in generating more cautious approaches to personal data disclosure. A behavioural approach based on changes to the choice architecture cannot and should not replace them. It can, however help them to get citizens to make choices that are in their best interest.

This study explored alternative ways of alerting users to the fact that their behaviour on-line revealed personal information about themselves. It measured their level of disclosure of personal information, as well as their replies to a questionnaire following exposure to different nudges.

Two types of personal information disclosure were considered: *passive*, when the user inadvertently reveals personal information (by simply browsing the Internet carelessly, for example), and *direct*, when the user purposefully reveals personal information (Groom & Calo, 2011). The distinction has policy implications. In passive disclosure, users are not aware they are disclosing personal information, and therefore do not take steps to regulate their information disclosure. Disclosure occurs inadvertently, out of users' awareness and control. In this case, privacy notices have little or no effect at all. Instead, this may be the right domain for a behavioural economics approach, since behaviour may simply be automatic and not the result of a thoughtful process.

The report first provides a literature review on current privacy policies and informed consent requirements as legal tools, and discusses some literature on behavioural science applied to public policy. It then presents the results of the experiment which tested the impact of different nudges on privacy behaviour. It also examines the possible influence of demographic variables such as age, gender, education and country of residence, and includes an analysis of self-reported measures such as perceptions of disclosure and feelings of being observed.

II. Background

In parallel to its key enabling role for economic growth and productivity, digital technology has spawned a new era in the disclosure of citizens' personal data. It represents a potential threat to privacy and data protection of the citizen, but also offers opportunities for strengthening them[1]. Reinforcing trust in the online environment is essential for the realization of the Internet's potential as an engine for European economic growth and innovation[2]. European Commission President Jean-Claude Juncker has stressed the need to 'make Europe more trusted and secure online, so that citizens and businesses can fully reap the benefits of the digital economy'.[3] This objective is also

[1] See Charter of Fundamental rights of the European Union, Art 7 and 8, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[2] European Commission, 2012

[3] http://ec.europa.eu/about/juncker-commission/docs/oettinger_en.pdf

recognised by the Digital Agenda for Europe (DAE)[4], the European Union flagship initiative on all ICT-related activities.

One way to reduce privacy concerns and increase trust is to provide users with good privacy policies which increase their awareness and reassure them about the risks involved (Wu, Huang, Yen & Popova, 2012). This should be done with caution, however, as offering greater privacy reassurances to individuals may lead to increased reluctance to reveal personal information by *priming* the individuals about the sensitivity of their data (Acquisti, 2010b). The role of privacy policies, therefore, should be to enable a cautious willingness to disclose personal data while at the same time safeguarding privacy and personal data protection (Europoean Commission, 2012).

The European Commission is addressing these challenges via the reform of the legal framework on privacy and data protection in the EU[5]. Directive 95/46/EC will be replaced by the General Data Protection Regulation, henceforth Draft Regulation, which aims to build a stronger and more coherent data protection framework in the EU (European Commission, 2012).

Privacy notices

Despite establishing these information obligations and consent requirements, the Draft Regulation contains few indications on *how* information should be provided to users or how they could exercise their right to object to the processing of their data. This means that, as far as the information provision obligations are satisfied, i.e. the minimum of information is provided, the controller is free to choose how to provide this information.

The common instruments usually adopted by data controllers to be compliant with the law are *privacy notices*. These are long, detailed and highly complex statements on how data controllers will use their personal data. These notices also provide information about the data subjects' rights and the security measures adopted for the safe treatment of their personal data. It is assumed that users read these texts, understand them and give their informed consent.

Individuals are given control of their personal data and expected to weigh the costs and benefits of the disclosure of their data themselves. This is an example of a *self-management* approach to privacy issues, whereby users are provided with information and expected to act according to their best interests (Solove, 2013).

These privacy notices have been gradually introduced, either through mandatory regulation (the case in the EU) or as self-regulation practices by businesses in response to privacy concerns (the case in the US). However, there are a number of problems with this approach.

Nobody reads privacy notices

Studies conducted both in Europe (Lusoli, Bacigalupo, Lupiáñez-Villanueva, de Andrade, Monteleone & Maghiros, 2012) and outside Europe (Tsai, Cranor, Acquisti & Fong, 2006; McDonald & Cranor, 2008) have shown that these notices are not effective. They are hard to read and read infrequently, least of all by young people (McDonald & Cranor, 2008; Madden, Lenhart, Cortesi, Gasser, Duggan, Smith & Beaton, 2013). Generally, users will scroll down the privacy notice and rush for the tick box, or simply tick the box without even looking at the notice (when this option is available). This habit does not allow them to give their meaningful, informed consent, and limits their ability to make 'rational' decisions.

---

[4] See EC Digital Agenda for Europe, available at http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

[5] The legal framework currently applicable in the field of privacy and data protection is represented mainly by Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* integrated by the Directive 2002/58/EC *concerning the processing of personal data and the protection of privacy in the electronic communications sector* (so called e-*Privacy* Directive, as modified by the Directive 2009/136/EC, the e-*cookies* Directive).

Information asymmetry

There is insufficient information for users to make a considered decision about data disclosure (Acquisti, 2010b). This is also referred to as 'information asymmetry' between users (they are unaware or they do not have enough information on what happens with their data) and data controllers (companies or government entities that collect and process users' data). Even if users received appropriate and clear information and knew how their data would be treated, they still would ignore the consequences of future data use (Borgesius, 2013). This knowledge asymmetry is exacerbated by the rise of *big data*.

Transaction costs

Transaction costs, namely the time needed for users to read and interpret privacy notices where complete information is provided, make information asymmetry even more difficult to overcome (Acquisti & Grossklags, 2007; McDonald & Cranor, 2008; Borgesius, 2013).

In addition, users face increasing uncertainty in online environments due to the new technological capabilities of tracking systems, which can be used in different ways by different actors to gather information[6]. In order to capture these changes, privacy policies change frequently though not always transparently, making the task of keeping abreast with the most recent version even more difficult for users (Martin, 2013). Transaction costs, therefore, increase.

Even well-informed and rational individuals sometimes cannot effectively self-manage their privacy due to several structural problems: (a) there are too many entities collecting and using personal data to make self-management based on the consent model feasible and (b) often privacy breaches are the result of an aggregation of pieces of data by different entities (Solove, 2013).

Privacy paradox

Internet users usually claim they are worried about online privacy risks and are aware of their privacy rights. Many are concerned that their personal data held by companies may be used for purposes other than those for which it was collected (Lusoli et al., 2012). However, most users do not act accordingly. They do not read the privacy policies entirely or they find it difficult to obtain information about a data controller's practices (Tsai, Cranor, Acquisti & Fong, 2006; Hoofnagle, King, Li & Turrow, 2010; Madden et al., 2013). Therefore, providing good, clear and accurate information about the risks of disclosing private information is not enough to change behaviour**.**

Favours the commercial use of data

Criticisms of the self-regulation model of privacy policies, in particular in the U.S., point to the fact that this model has allowed a sectoral and weak approach to privacy (Solove & Hoofnagle, 2006) which favours the commercial use of personal data. As a result, privacy policies without substantial safeguards have proliferated. Individual protection has become an illusion rather than a reality: users may believe they have more privacy simply because a website has a privacy policy (Haynes, 2007).

In sum, current privacy policies which 'take refuge in consent' do not provide people with meaningful control over their data (Solove, 2013). Consent in these circumstances is insufficiently informed and, therefore, generally not meaningful (Borgesius, 2013). Current policies fall short of achieving the objectives of law, namely to ensure that people make considered decisions about their privacy, and, ultimately, to increase trust in on-line services.

---

[6] See Ashkan Soltani's work for an excellent overview of different methods that are used to track users: http://ashkansoltani.org/work/online-tracking.

Alternative mechanisms to traditional privacy policies

As users very often do not read privacy policies, other strategies might be more successful in encouraging privacy-protective behaviour. Instead of only using written privacy policies, organisations could embrace alternative ways and instruments – more visual, explicit, simple and user-friendly – to inform Internet users so that they give better-informed consent, if they give it.

- *Transparency enhancing tools* (TETs) would allow citizens to anticipate how they will be profiled and what the consequences of this would be (Hildebrandt, 2012). Tools such as Ghostery, Privacy Badger and other browser extensions make online tracking more transparent and give users the technological means to block trackers. However, not everyone knows about TETs, and not everyone can use them or is interested in doing so. They do require people's conscious attention and they do require a certain amount of cognitive effort. This takes us back to some of the problems encountered with privacy notices.
- One alternative is to provide simplified, *standardized privacy information*. These are notices which convey a simple message in a standardized format, such as the cookie alerts required by the EU. This approach has some benefits. For one, the messages are shorter and easier to understand. However, they can also prove to be insufficient, as users may end up ignoring these alerts and simply accepting all the requests for consent with a click of the mouse button, as a matter of habit (Groom & Calo, 2011).
- Finally, a *privacy by design* approach (PbD) (Cavoukian, 2012) advocates good technical design which embeds privacy into IT systems and business practices from the outset (and doesn't just add privacy measures ex-post). It proposes seven 'foundational principles' to offer the highest degree of privacy to individuals. These include, for example, ensuring that personal data are automatically protected by default, being preventative and not remedial, and always keeping the interests of the end user in mind (i.e. remaining user-centric).

Nudging privacy behaviour

Empirical findings about human behaviour are increasingly being taken into consideration by policy-makers worldwide and incorporated into policy initiatives across different policy areas (Sunstein, 2000; Shafir, 2013; van Bavel, Herrmann, Esposito and Proestakis, 2013; Lunn, 2014; World Bank, 2015). These findings are commonly applied to improving the background against which people make their decisions (the *choice architecture*; Thaler & Sunstein, 2008). Policy-makers effectively become choice architects, making appropriate and small changes in the underlying environment that may have a large impact on people's behaviour. In an on-line environment, the choice architecture includes features such as website design, warnings, and defaults (Sunstein, 2013).

An important behavioural insight is that the more our activities are routinized, repeated on a daily basis, the more people *think fast* (Kahneman, 2011). This is particularly interesting for daily digital activities, involving e-mail or Internet browsing, for example. Such activities are often repetitive and systematic gestures. This is also true of on-line terms and conditions, or privacy notices, which we very often accept without reading. Changing them requires the appropriate tools which tap into this automatic behaviour, not tools that require effort and deliberation by the user.

This study aims to identify and test *privacy nudges* (Acquisti, 2009; Acquisti, 2010a; Acquisti, Brandimarte & Loewenstein, 2015; John, Acquisti & Loewenstein, 2009; Wang, Leon, Scott, Chen, Acquisti & Cranor, 2013), similar to *visceral notices* (Calo, 2012; Groom & Calo, 2011), as alternative and complementary measures for personal data protection[7]. Privacy nudges are not meant to replace the notice and choice system *per se*, but rather to improve it and provide more suitable, flexible and effective privacy-protective mechanisms.

[7] See Calo (2014) for a detailed discussion of the difference between a code, a nudge and a notice in privacy behaviour.

Unlike traditional privacy notices that rely on text or symbols to convey information, nudges or visceral notices 'leverage a consumer's very experience of a product or service to warn or inform' (Calo, 2012). Previous experiments on visceral notices (Groom & Calo, 2011) not only demonstrated the weaknesses of traditional explicit notices, but also that other notice strategies can be successful at eliciting privacy-protective behaviour. This study builds on these results and follows the same empirical tradition.

III. Research design

The study is based on an on-line experiment inspired by Groom and Calo's (2011) research, but with a much larger sample (3,229 participants) and in more countries (Germany, Italy, the UK and Poland). This selection allowed us to get results from the north, south, east and centre of the EU.

Data collection

The data were collected between March and June 2014 by Harris Interactive under the guidance of University Tor Vergata. Harris first prepared a sample plan for recruiting a representative group of participants from four European countries. Then, based on the sample plan, they set quotas to balance demographic variables and performed real-time quota management during the run of the study. All participants were randomly assigned to one of the seven experimental conditions or the control group. In order to participate in the survey, participants had to:

- Be at least 18 years old
- Be connected to the Internet from the appropriate country, among the four countries chosen for the study
- Have a reliable Internet connection

A pilot with 263 participants (assigned randomly to the various conditions) was run before the actual experiment, using Amazon MTurk. This allowed for changes and adjustments in the design of the experiment.

Experimental protocol

Participants were assigned to one of the seven experimental conditions (or the control group) and asked to use and then evaluate a mock search engine. However, this was a pretext – the real purpose of the experiment was to observe their behaviour. The study targeted around 400 subjects per experimental condition and around 100 subjects per experimental condition per Member State.

The internal Evaluation Committee set up at the Institute for Prospective Technological Studies approached this study as an on-line split ballot questionnaire and sought adherence to the appropriate ethical guidelines for conducting surveys. Informed consent was obtained from all participants in the study, according to the Terms of Services and Privacy Policy of Harris Interactive[8]. Participants were debriefed about the purpose of the study at the end of the experiment.

The mock search engine was capable of searching for the answers to a set of sixteen pre-established questions. This mock search engine merely consisted of a website interface; no actual search technology was created. In other words, the search engine website interface simply connected to an existing search engine (Google).

The mock search engine had an ad-hoc name ('Re-Search Engine'), a logo, a search box and, below, an area displaying search results. The search engine interface was translated into the languages of

[8] These documents cover issues ranging from confidentiality to consent and voluntary participation: https://join.harrispollonline.com/?sid=068bbad9-0651-46dc-8083-08eecfcf7aed#

the four countries selected. It was also adapted and modified according to the needs of the seven experimental conditions or control group described in the next section.

The mock search engine could direct participants to existing external webpages. However, it was ensured that the subjects returned to the mock search engine website once they had found the answers to the search queries, so that they continued with the experiment. The questions that the participants were asked were displayed above the search box. Below the search box, another box was provided in which participants could type their responses.

The fact that the study's setting was somewhat artificial might have had an impact on absolute results. Participants were aware that they were participating in a study, and knew that their privacy would in fact always be guaranteed by the Privacy Policy of Harris Interactive, with whom they had signed a prior agreement. This might have led them to disclose more personal information that would have normally been the case. However, results in an experiment will never accurately reflect behaviour in the 'real world'. The objective, therefore, should be to observe the *comparative* impact of different treatments on behaviour, not their absolute impact. This comparison should not be subject to bias, since all experimental conditions are subject to the same overall environment.

Finally, at the end of the experiment the software displayed separate pages, with the questionnaires on Internet use and on the user interaction with the search engine. The questionnaires were also translated into all the languages of the four selected EU Member States.

The experiment lasted an average of twenty-three minutes. Participants were asked to use the search engine to find the answers to four general knowledge questions. These searches allowed for the collection of information on the IP address of participants' computers, the web browser used and web pages that were visited (which would be relevant later on). Participation in the experiment could not be discontinued, otherwise it would be considered invalid.

Experimental conditions

The eight experimental conditions closely followed the experimental conditions first used by Groom and Calo (2011). However, unlike Groom and Calo, all conditions, except for the control group, included a link to a privacy notice. This is more in line with the European Data Protection regime and with the current practices of existing websites, and allowed us to compare like and like. Had we included a privacy notice link in some conditions and not others, we would not have been able to assign causality to a single variable. This would also allow for testing users' willingness to read privacy policies, whether simplified or not, after a treatment. The eight experimental conditions were as follows (see illustrations in Annex 1):

- Control: The search engine did not include any privacy notice. Otherwise it displayed the same appearance as the other conditions (except for the informality condition). Nuances of blue or grey were used throughout the webpages to transmit authority and seriousness.
- Traditional: This experimental condition displayed a clickable privacy policy link at the top of the far-right column. Clicking the link would open a page displaying a traditional privacy notice, consisting of written text, explaining precisely what data were going to be collected by the mock search engine and how these data would be used.
- Simplified: This experimental condition displayed the same link to a privacy notice as in the *traditional* condition, but which led to a much simpler version of the same notice. The same information was conveyed in simpler language and with the help of a table.
- Static agent: An anthropomorphic character displayed from the shoulders up which appeared in the right column in line with the search box with a text written below. Participants were able to see a static image of this agent with the words 'what would you like to search for?' beneath it. The agent had the appearance of a customer service agent.
- Interactive agent: Included the same anthropomorphic character and the same text as in the *static agent* condition, but with moving head and eyes tracking cursor movements.

- Informality: The overall appearance of the search engine website was adjusted to convey a more informal and youthful look and feel than the others. It had bright yellow background with green and blue accents and red text, with softer lines in the logo and title, rounded shapes for the buttons and Comic Sans font. The content and structure were the same as the other seven conditions.
- IP information: This condition displayed the participants' real IP, location and the browser that they were using on the right side of the search engine webpage. The three corresponding messages were: "Your IP is [...]"; "Your current location is [...]"; "Your current browser is [...]". This information was collected for all participants and explained in the privacy policy, though it was only visibly displayed to the participants in this condition.
- History: This condition displayed the URL of each external website visited during the search experience on the right side of the search engine webpage. This information appeared in line with the search box. When participants visited a new site, the corresponding URL appeared at the top of the list. Click-stream data were collected for all participants and this was clarified in the privacy notices, though it was visibly displayed only to the participants in this condition.

Behavioural output measures

The experiment measured two types of personal data disclosure by participants: *passive and direct*.

- Passive disclosure was measured by the number of 'sensitive' questions answered. Participants were shown four sets of three questions in sequence and asked to find the answer to one of the questions in each set. This led to a total of four questions being answered. In each of the four sets, the answer to one of the questions would reveal (albeit indirectly) personal information, such as information on participants' bank, their home town or their year of birth (e.g. 'what year was your bank founded?'). The other questions did not require the user to reveal any personal information whatsoever. Participants' choice of question to answer is therefore a measure of their passive disclosure of personal information.
- Direct disclosure was measured by the number of questions answered about engaging in socially stigmatised behaviour[9]. Participants could answer *never*, *once or twice*, *sometimes*, or *frequently*, but – crucially – they also had possibility to not answer at all. In other words, responding was optional. The number of times that the respondents decided to answer such questions, despite being optional, formed the basis for the measure of direct disclosure[10].

Questionnaire

Complementary measures were collected through the responses to a number of additional questions (see Annex 2), structured as follows:

- Participants' usual internet usage[11].
- Participants' interaction with the search engine site. The possible answers here were structured in a 7-point Likert scale and ranged from *strongly disagree* to *strongly agree*[12]. The purpose was to have additional results on perceived difference with a real search engine to see how it changed according to experimental condition.
- Items related to the search engine, aiming to verify users' level of awareness of online tracking practices and of privacy concerns. The possible answers were also structured in a 7-point Likert scale from *strongly disagree to strongly agree*[13].

---

9 E.g. 'Have you ever looked at pornographic material?'

10 Providing false data is also a common privacy strategy, but since responding was optional, it was assumed respondents did not have to resort to that.

11 E.g. 'What browser do you typically use?'

12 E.g. 'Do you think the search engine you tested is easier to use than the search engine that you typically use?'

13 E.g. 'The search engine website was able to detect several pieces of information about my online activity.'

- Items aimed at measuring whether participants had noticed some elements during the experiment, even in the case where these elements were not present at the website[14]. The purpose was to test whether noticing these elements may affect their predisposition to disclose personal information.
- Socio-demographic data (e.g. age, education level, and current employment situation).
- Exit questions relating to the goal of the study, the device they used to take the survey, etc.

IV. Results

Sample characteristics and socio-demographics are presented in detail in Annex 3.

Behavioural output measures

Passive disclosure

The experiment originally included four sets of three questions for measuring passive disclosure. However, in preliminary analyses one of these sets showed a disproportionate number of participants choosing to answer the sensitive question compared to the other sets. The question was 'what is the street address of a post office in the town where you live?', and 64% of subjects chose to answer it. In the other sets, the personal questions were chosen by 24%, 30% and 19% of subjects. This was puzzling, and might have been due to the fact that this question required no search, as people are often familiar with the street of their local post office. For this reason, the set was omitted from subsequent analyses.

A probit model was used to test differences in passive disclosure[15]. Choosing to answer at least one sensitive question scored 1; not choosing any sensitive questions scored 0. In the model, the dependent variable was passive disclosure, and the independent variables were *treatment, country, gender, education level* and *age* (see Table 1).

Experimental treatments

Participants assigned to the *static anthropomorphic* condition disclosed more personal information than participants in the rest of conditions. Almost 60% of them chose to answer at least one personal question (Figure 2). They were followed by participants in the *dynamic anthropomorphic* condition (57% chose to answer at least one personal question).

The probit regression confirms these results: the only experimental treatments that had an effect on passive disclosure were *static* and *dynamic anthropomorphic* characters. Subjects who visualized these characters were more likely to answer questions that revealed personal information than subjects in the *control group* (see Table 2). In the *static anthropomorphic* condition, this difference is significant at a 95% confidence level; in the *dynamic anthropomorphic*, at a 90% level (Table 2).

This result may be explained by the fact that, as demonstrated elsewhere in the literature, anthropomorphic images increase trust in on-line transactions (e.g. Bente et al., 2014). And with this increased trust comes less vigilant behaviour which leads to inadvertent disclosures of personal information.

[14] E.g. 'While you were answering the quiz questions, did you notice an IP address?'

[15] The aim of the probit model is to estimate the probability that an observation with particular characteristics will fall into one of two categories.

Table 1: Probit regression for passive disclosure with Control and Italy as baselines for treatment and country

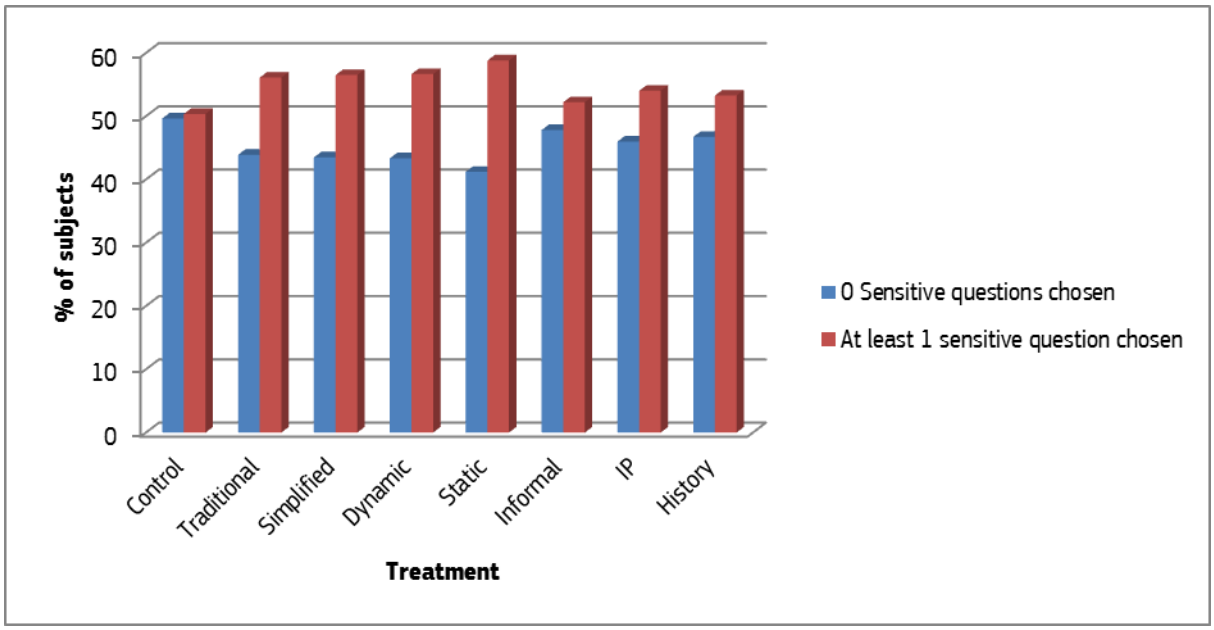
	VARIABLES	Passive Disclosure
Treatment	Traditional	.1241855
	Simplified	.1404511
	Anthropomorphic Dynamic	.1616479*
	Anthropomorphic Static	.2036759 **
	Informal	.0327754
	IP	.0758884
	History	.0562358
Country	Germany	-.3469802***
	Poland	-.3338886***
	UK	-.3709523***
Other	Gender	.0225792
	Education level	-.1060172***
	Age	.084415**
	Constant	-.0576963

*** p<0.01, ** p<0.05, * p<0.1*

Treatment: Control = 1; Country: Italy = 1; Gender: Female = 1; Education level: College attendees = 1

Age: >42 = 1

Figure 2: Subjects' passive disclosure by treatment in percentage



Country of residence

Participants in Italy revealed more personal information inadvertently: almost a 65% of them chose to answer at least one of the sensitive items. On the other hand, in the other three countries (Germany, Poland and the UK) between 48-49% of the subjects were able to avoid revealing personal information in this way (Figure 3). Table 3 shows information on how many participants chose to answer more than one of the sensitive items. In Italy, more subjects chose all 3 sensitive items.

In the probit model, taking Italy as the baseline country, there is a statistically significant difference between participants in this country and those in Germany, Poland and the UK ($p < 0.001$, Table 2). No other significant country differences were found.

Figure 3: Subjects' passive disclosure by country in percentage

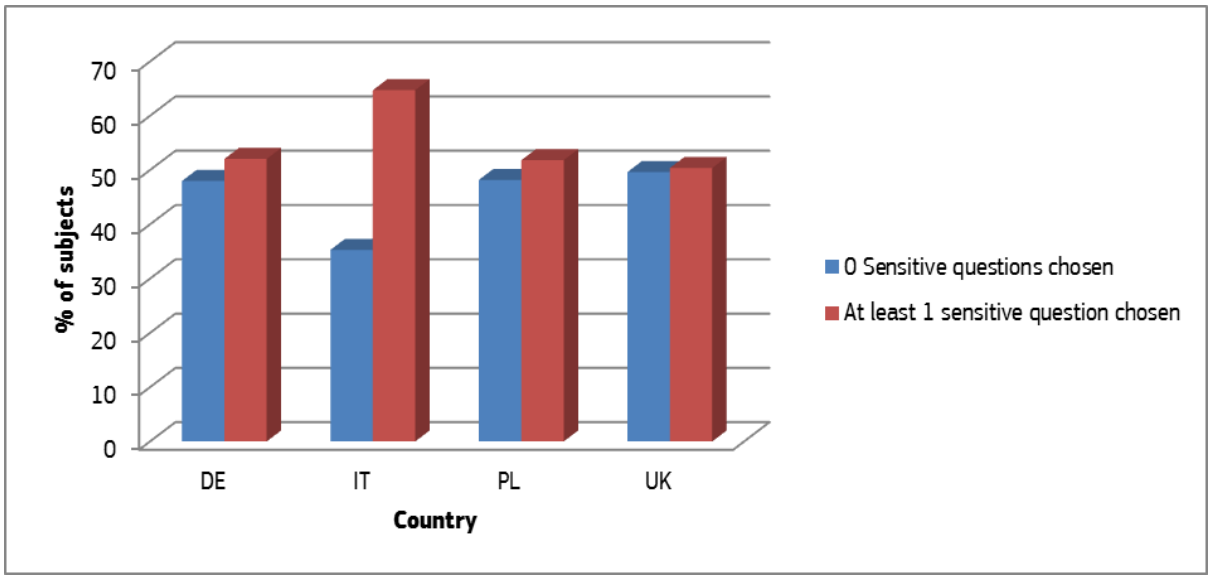


Table 2: Passive disclosure by Country: number of sensitive items answered

Country	0	1	2	3	Total
Germany	390	293	117	13	813
Italy	282	304	169	44	799
Poland	387	302	91	23	803
UK	404	314	87	9	814
Total	1,463	1,213	464	89	3,229

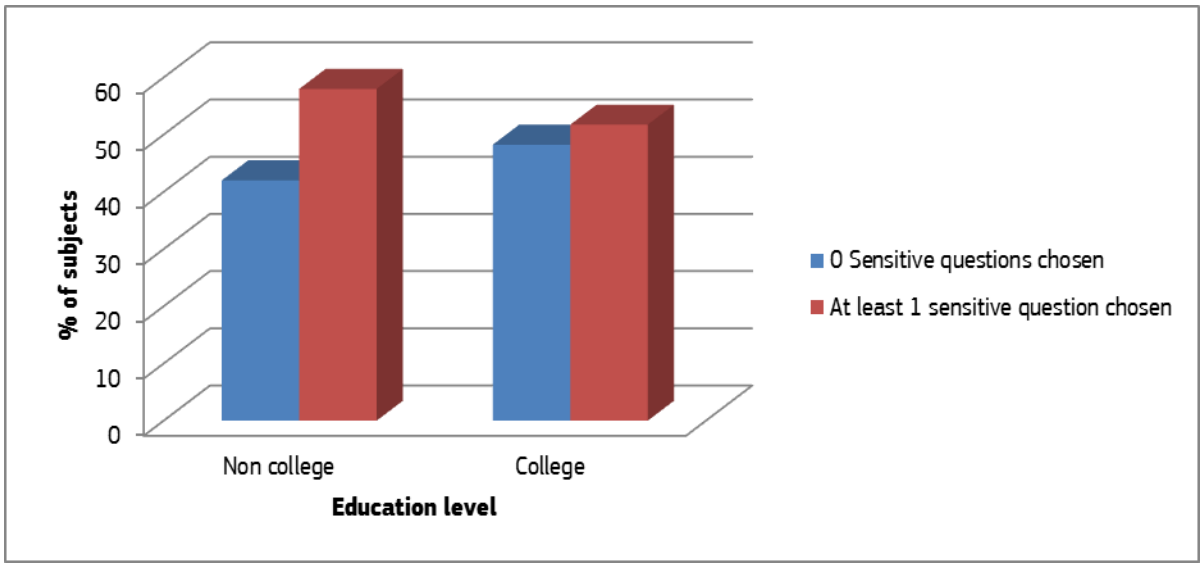
Gender

No significant differences were found for passive disclosure according to gender (Table 2).

Education

For analytical purposes, subjects were merged into two categories: those who had at least attended college and those who never attended college. Participants who had a higher level of education were less likely to answer sensitive items ($p<0.001$; Table 2). 48% of the more educated group avoided answering sensitive questions, compared to 42% of less educated participants.

Figure 4: Subjects' passive disclosure by education level in percentage

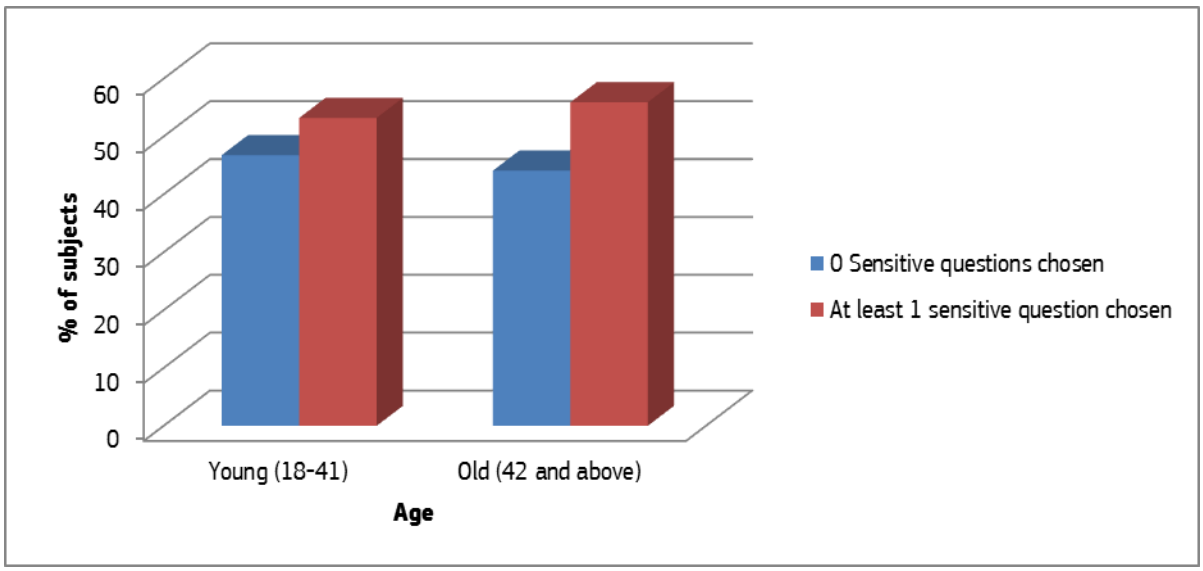


Age

Participants were split into two groups with the objective to compare between younger vs. older individuals). The 'younger' group included participants between 18 and 41 years old. The 'older' group included subjects who were 42 years old or more. The option "I prefer not to answer" was also registered.

The results of the probit model show that older participants passively revealed more information than younger participants ($p < 0.05$; Table 2). Almost 56% of them chose to answer at least one personal question, compared to 53% of younger participants (Figure 5).

Figure 5: Subjects' passive disclosure by age in percentage



Direct disclosure

The results of the impact of treatments on direct disclosure were measured with a Poisson model, in which the dependent variable (direct disclosure) is a count. The possible outcomes were to answer positively to 1 to 10 stigmatised behaviours or not to answer any of them, or answer negatively (i.e. 'never') to all of them, scoring 0. In the proposed model, the dependent variable is direct disclosure, and the independent variables are treatments, country, gender, education level and age (see Table 3).

Table 3: Poisson regression for direct disclosure with Control and Italy as baselines for treatment and country

	VARIABLES	Direct Disclosure
Treatments	Traditional	.0670005*
	Simplified	.0315333
	Anthropomorphic Dynamic	.0688383*
	Anthropomorphic Static	.0639918
	Informal	.0201771
	IP	.0206437
	History	.0555555
Country	Germany	.1450458***
	Poland	.3489893***
	UK	.2063947***
Other	Gender	-.185638***
	Education level	-.0199921
	Age	-.0816732***

**** p<0.01, ** p<0.05, * p<0.1*

Treatment: Control = 1

Country: Italy = 1; Gender: Female = 1; Education level: College attendees = 1; Age: >42 = 1

Treatments

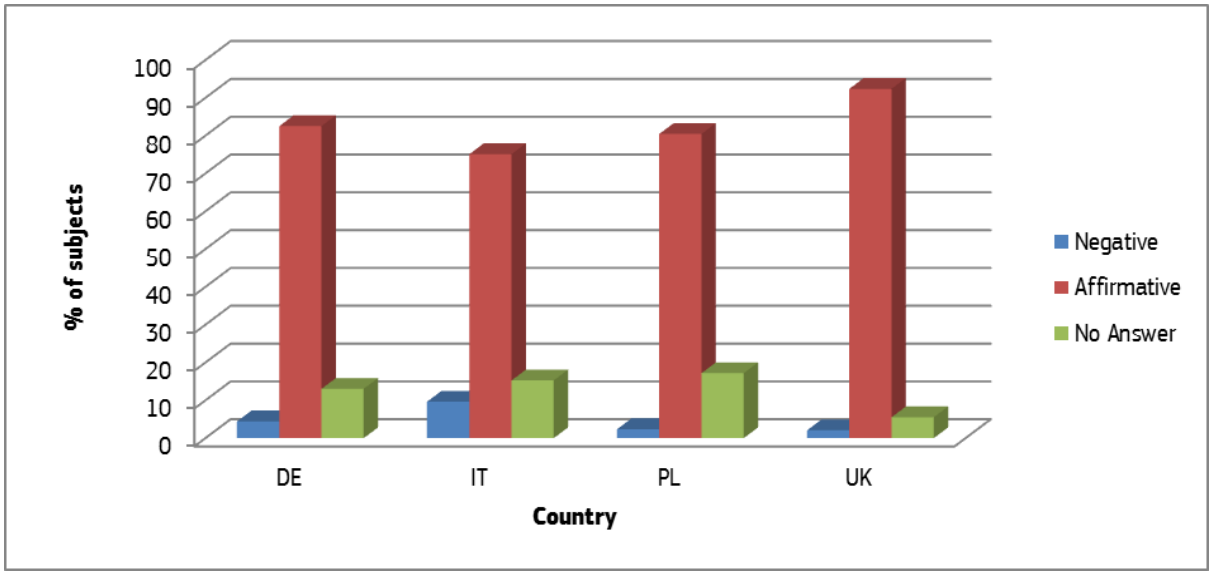
The results reveal that, subjects who visualized the *anthropomorphic* character in its *dynamic* condition were more likely to answer stigmatised personal questions compared to the *control* group ($p < 0.10$; Table 3). This outcome partially corroborates the results obtained for *passive disclosure*. It would seem that anthropomorphic images increase subjects' predisposition to disclose personal information, either wittingly or unwittingly.

However, the *traditional* treatment (displaying a clickable privacy policy link) also shows a positive coefficient which is significant at a 90% level of confidence (Table 3). Subjects exposed to a privacy link, without an additional nudge, in the search engine revealed more personal information than subjects who did not see a privacy link (*control* treatment). Perhaps, seeing a privacy policy link reassured participants and made them believe that their answers would not be shared, as people often think of a privacy policy as some kind of guarantee of privacy (Hoofnagle and King, 2008). However, this should have also applied, to a certain degree, to others who saw the privacy link alongside other nudges.

Country

Even though participants in Italy revealed the most personal information in *passive disclosure*, in *direct disclosure* they revealed less than the other countries. Approximately 75% of participants in Italy chose to answer positively to at least one stigmatised question, compared to 81% in Poland, 83% in Germany and 92% in the UK (Figure 6).

Figure 6: Subjects' direct disclosure by country in percentage



Gender

Female participants directly disclosed less information about personal and stigmatised behaviour than men ($p<0.001$; Table 3). Approximately 73% of women answered 'never' to the stigmatised questions (males 27%; Figure 7). Women were also more likely to avoid answering to this set of items: 57% compared to a 43% of men (Table 4).

Figure 7: Subjects' who answered "Never" to all the direct disclosure items

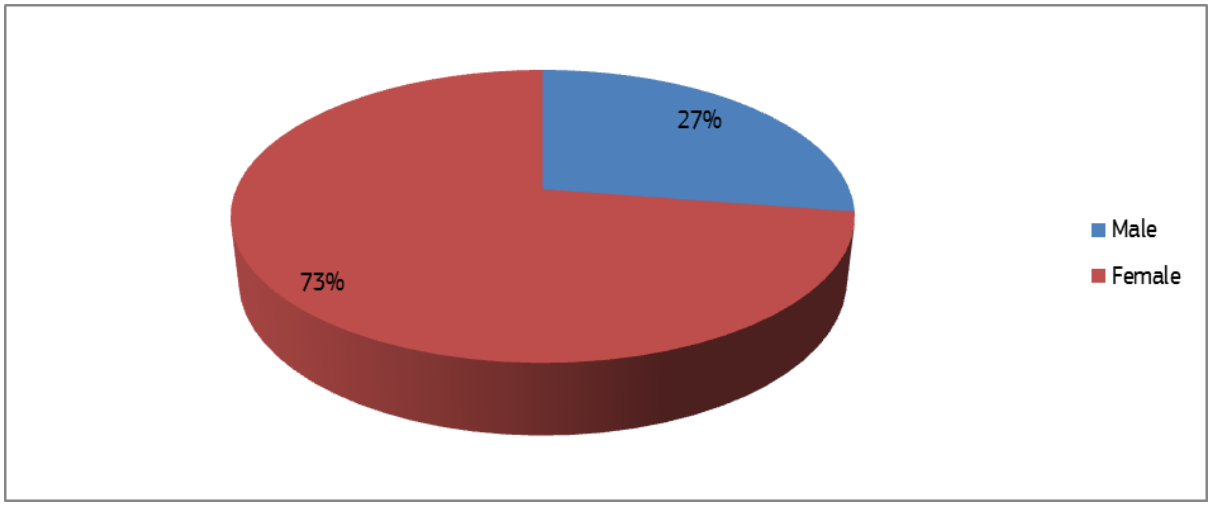


Table 4: Direct disclosure by gender: percentage of subjects by type of answer (%)

	Answered Never	Answered Affirmatively (to at least one question)	No Answer
Male	27.46	51.87	43.18
Female	72.54	48.13	56.82

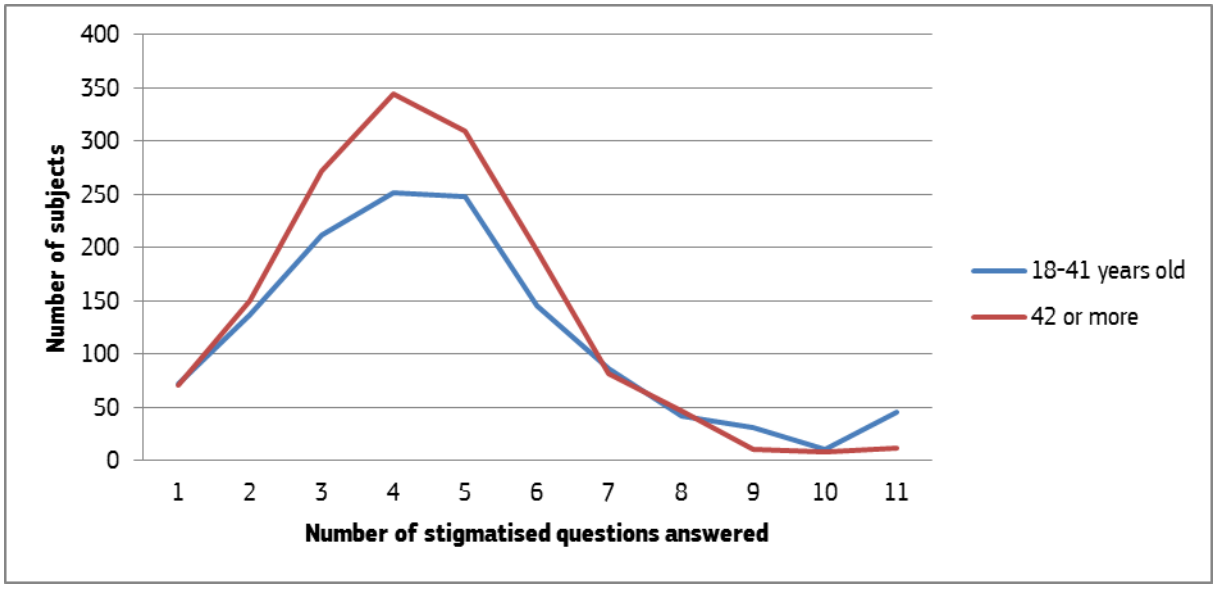
Education

No significant differences were found for direct disclosure according to education (Table 3).

Age

The Poisson analysis shows that the group of participants aged 42 and above revealed less stigmatised information ($p<0.001$; Table 5) than the younger group. Although a greater number of older participants answered positively to 6 or fewer stigmatised questions, a greater number of younger subjects answered 8 or more stigmatised questions (Figure 8). These results are contrary to those of passive disclosure, where older participants revealed more information.

Figure 8: Subjects' direct disclosure by age in absolute value



The results confirm that passive and direct disclosure are two different constructs, intended to capture different ways of revealing personal information. Indeed, the correlation between both is very low (Table 5).

Table 5: Correlation between passive and direct disclosure

	Passive disclosure	Direct disclosure
Passive disclosure	1.0000	
Direct disclosure	0.0253	1.0000

Self-reported measures

In addition to the measures of behaviour outlined above, the experiment included a questionnaire. The questionnaire items sought to capture (a) *disclosure perception*, i.e. subjects' awareness that the quiz questions could reveal personal information about themselves, (b) *feeling of being observed / monitored*, i.e. whether subjects felt their on-line behaviour was being tracked and their degree of comfort in answering questions as a consequence and (c) *privacy policy link awareness*, i.e. whether subjects saw the link to a privacy notice. Since the questionnaire was completed after exposure to the experimental treatments, these constructs could have also been affected by them.

Disclosure perception

This construct was measured by a single item ('my answers to the quiz questions revealed personal information about myself'). Subjects indicated their agreement with the statement on a seven-point Likert scale ranging from 'strongly agree' to 'strongly disagree'. An ordered probit model tested differences for this item (Table 6)[16]. *Treatments*, *country, gender, education level* and *age* were introduced as independent variables in the model (see Table 6).

Table 6: Ordered probit regression for disclosure perception with Control and Italy as baselines for treatment and country

	VARIABLES	Disclosure Perception
Treatments	Traditional	.0278351
	Simplified	-.0052195
	Anthropomorphic Dynamic	-.0024431
	Anthropomorphic Static	-.0123343
	Informal	.0208297
	IP	-.0796003
	History	.0652004
Country	Germany	.3857499***
	Poland	.3367445***
	UK	.0541955
Other	Gender	.1104099***
	Education level	.0902366***
	Age	-.0157353

*** p<0.01, ** p<0.05, * p<0.1

Treatment: Control = 1; Country: Italy = 1; Gender: Female = 1; Education level: College attendants = 1; Age: >42 = 1

Treatments

No significant effect for *disclosure perception* was found according to experimental treatments.

Country

In Germany, subjects perceived more information disclosure (M = 5.16, SD = 1.79), followed by subjects in Poland (M = 5.05; SD = 1.91), the UK (M = 4.62; SD = 1.83) and Italy (M = 4.50; SD = 1.89). Figure 9 compares means for disclosure perception.

[16] Ordered probit is a generalisation of the probit analysis to cases with more than two outcomes of an ordinal dependent variable.

The ordered probit analysis shows that subjects in Italy were least likely to believe they had disclosed information compared to those in Germany and Poland ($p < 0.01$). However, there was no significant difference compared to those in the UK (Table 6).

When the baseline country for the ordered probit regression was changed from Italy to Germany, subjects from the UK were less likely to perceive they had disclosed personal information compared to subjects from Germany ($p < 0.01$). The same happened when Poland was taken as a baseline country (Table 7): subjects from the UK were less likely to believe they had disclosed personal information ($p < 0.01$). No significant differences were found between Germany and Poland.

Figure 9: Mean level of disclosure perception by country of residence

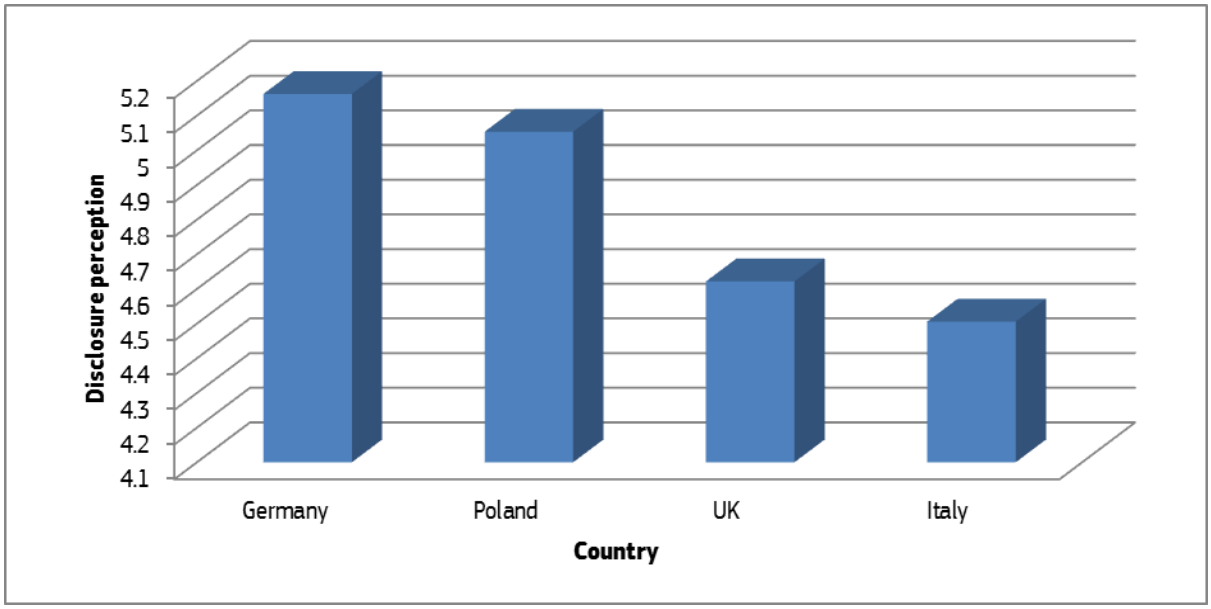


Table 7: Ordered probit regression for disclosure perception with Germany as baseline country

	VARIABLES	Disclosure perception
Country	Italy	-.3857499***
	Poland	-.0490054
	UK	-.3315544***

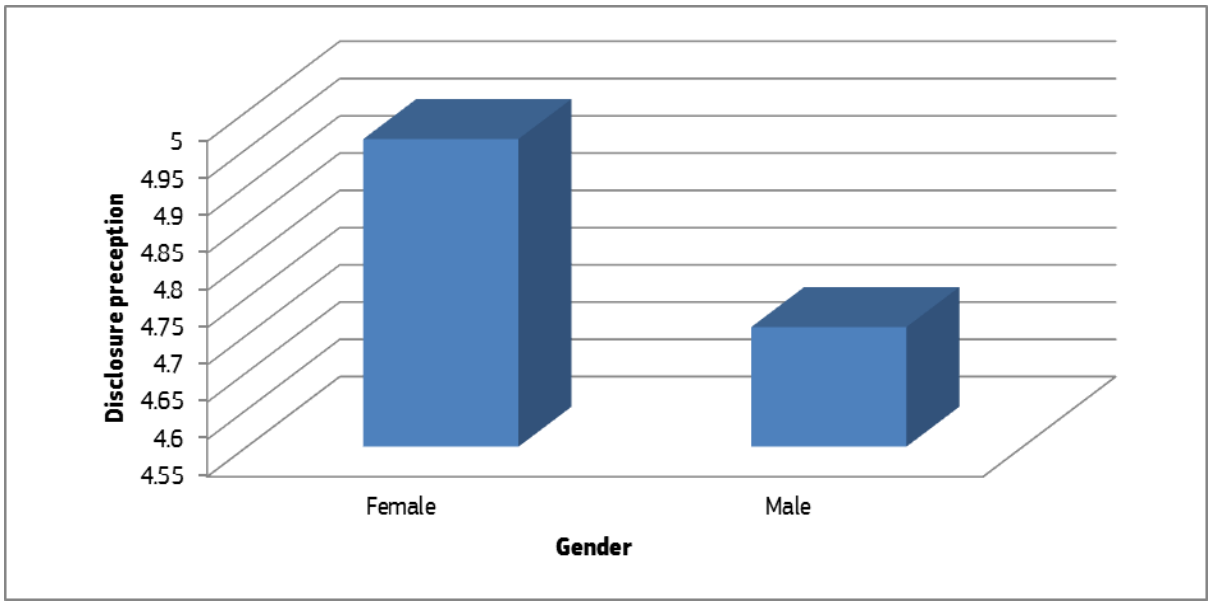
Table 8: Ordered probit regression for disclosure perception with Poland as baseline country

	VARIABLES	Disclosure perception
Country	Germany	.0490054
	Italy	-.3367445***
	UK	-.282549***

Gender

Women were more likely to believe their answers to the quiz questions revealed personal information about themselves ($p < 0.01$, Table 6). Figure 10 shows mean level of disclosure perception by gender (women: M = 4.9; SD = 1.87; men: M = 4.7; SD = 1.87).

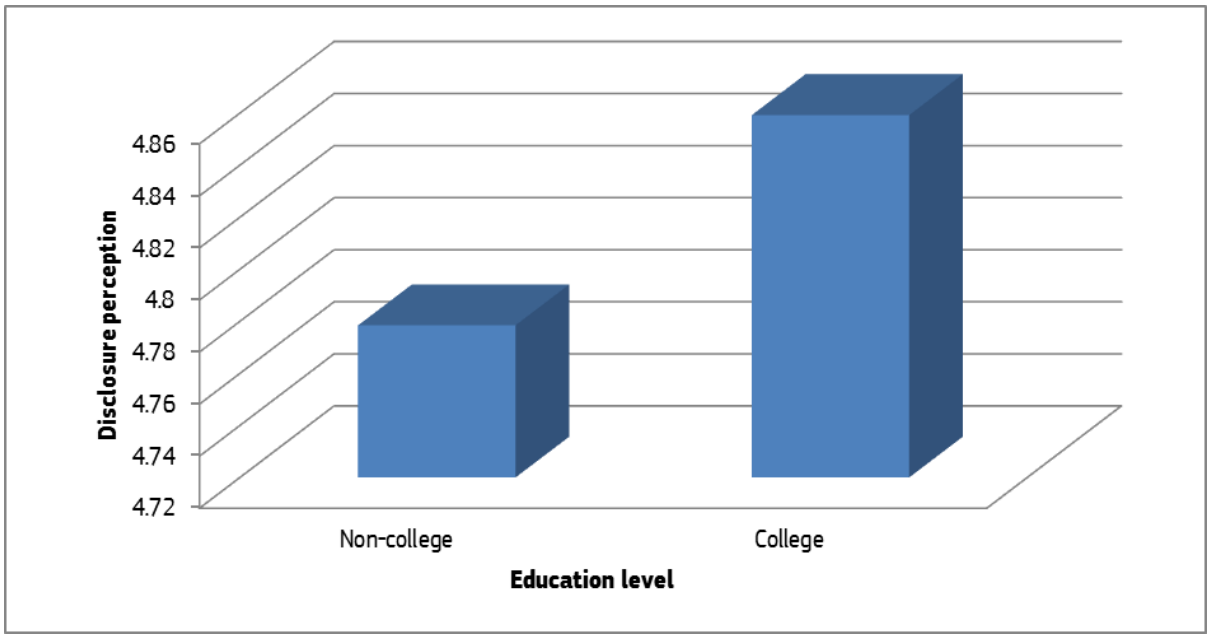
Figure 10: Mean level of disclosure perception by gender



Education

Subjects with a higher level of education perceived they had disclosed more information than those with a lower level of education ($p < 0.01$; Table 6). Subjects who had attended college had a higher mean level (M = 4.86; SD = 1.90) than those who had not (M = 4.78; SD = 1.85; Figure 11).

Figure 11: Mean level of disclosure perception by education level



Age

No significant effect for *disclosure perception* was found according to age.

Feeling of being observed / monitored

This construct was measured by three items: 'I felt comfortable answering personal questions during this study' (Q36, reversed), 'I felt observed during this study' (Q37), and 'I felt I was being monitored during this study' (Q38). Participants rated each item on a seven-point Likert scale ranging from 'strongly disagree' to 'strongly agree'. The higher this construct scores, the more they felt their actions were noted while participating in the experiment.

Table 9: Correlation between items of the feeling of being observed / monitored

	Q36	Q37	Q38
Q36	1.0000		
Q37	0.2878	1.0000	
Q38	0.2984	0.8165	1.0000

Table 10: Ordered probit regression for the feeling of being observed / monitored with Control and Italy as baselines for treatment and country

	VARIABLES	Feeling of being observed / monitored
Treatments	Traditional	-.0176888
	Simplified	.0507388
	Anthropomorphic Dynamic	-.060725
	Anthropomorphic Static	.0399455
	Informal	-.0080207
	IP	-.0411596
	History	.0734501
Country	Germany	.3933074***
	Poland	.0842225*
	UK	.1820166***
Other	Gender	-.1661339***
	Education level	-.2312539***
	Age	.1587669***

**** p<0.01, ** p<0.05, * p<0.1*

Treatment: Control = 1; Country: Italy = 1; Gender: Female = 1; Education level: College attendants = 1; Age: >42 = 1

The latent variable *feeling of being observed / monitored* presents high reliability (α = 0.7285)[17]. Eliminating item 36 increased the reliability of the construct (α = 0.8989). However, that item was

[17] Hinton, Brownlow, McMurray & Cozens (2004) suggest four cut-off points, which involve excellent reliability (0.90 and above), high reliability (0.70-0.90), moderate reliability (0.50 -0.70), and low reliability (0.50 and below).

kept in order to ensure the robustness of results. Correlations were very high between item 37 and item 38 (0.8165), but lower between 37 and 36 (Table 9).

An ordered probit model tested for differences in this construct, where *treatments*, *country, gender, education level* and *age* were introduced as independent variables (Table 10). The control condition and Italy were the baselines for treatment and country.

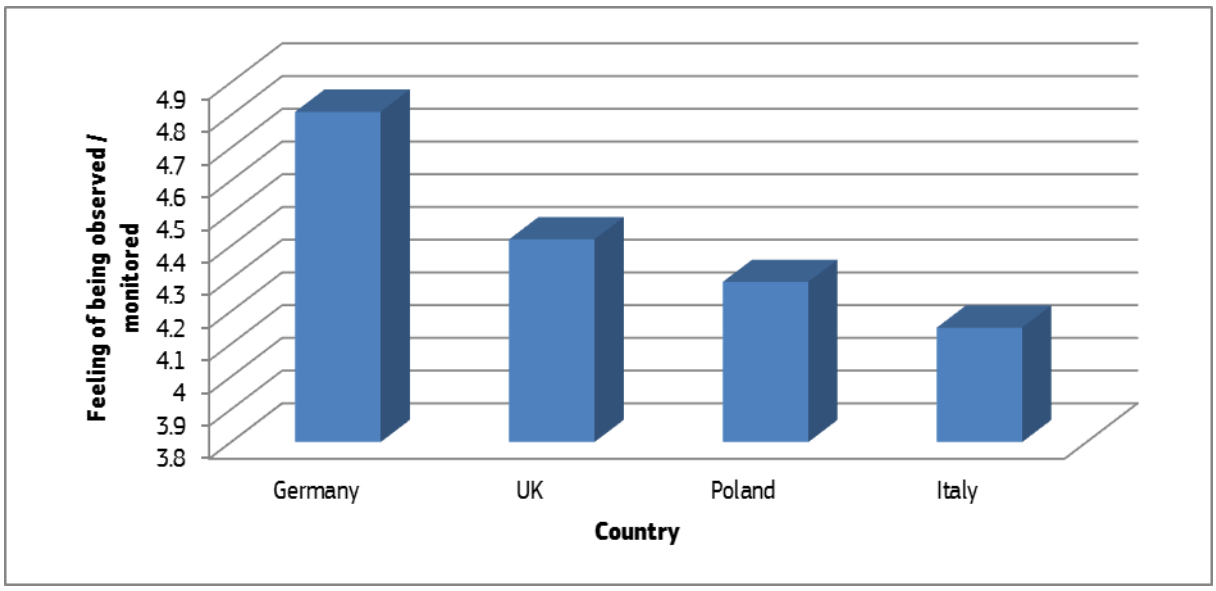
Treatments

No significant effect for *feeling of being observed / monitored* was found according to experimental treatments.

Country

In Italy, subjects felt less monitored while using the website (M = 4.15, SD = 1.54), followed by Poland (M = 4.29; SD = 1.62), the UK (M = 4.42; SD = 1.34) and Germany (M = 4.89; SD = 1.55) (Figure 12).

Figure 12: Mean feeling of being observed / monitored by country of residence



Participants in Italy did not feel they were being observed (Table 10) as much as those in the rest of the countries ($p < 0.01$ for Germany and the UK; $p < 0.1$ for Poland).

If Germany is taken as baseline country, subjects from Poland and the UK seem to feel less monitored or observed than participants from Germany ($p < 0.01$; Table 11).

When taking Poland as the reference, there are also significant differences showing that subject from the UK felt more monitored than those in Poland ($p < 0.01$; Table 12).

Table 11: Ordered probit regression for the feeling of being observed / monitored with Germany as baseline country

	VARIABLES	Feeling of being observed / monitored
Country	Italy	-.3933074***
	Poland	-.309085***
	UK	-.2112908***

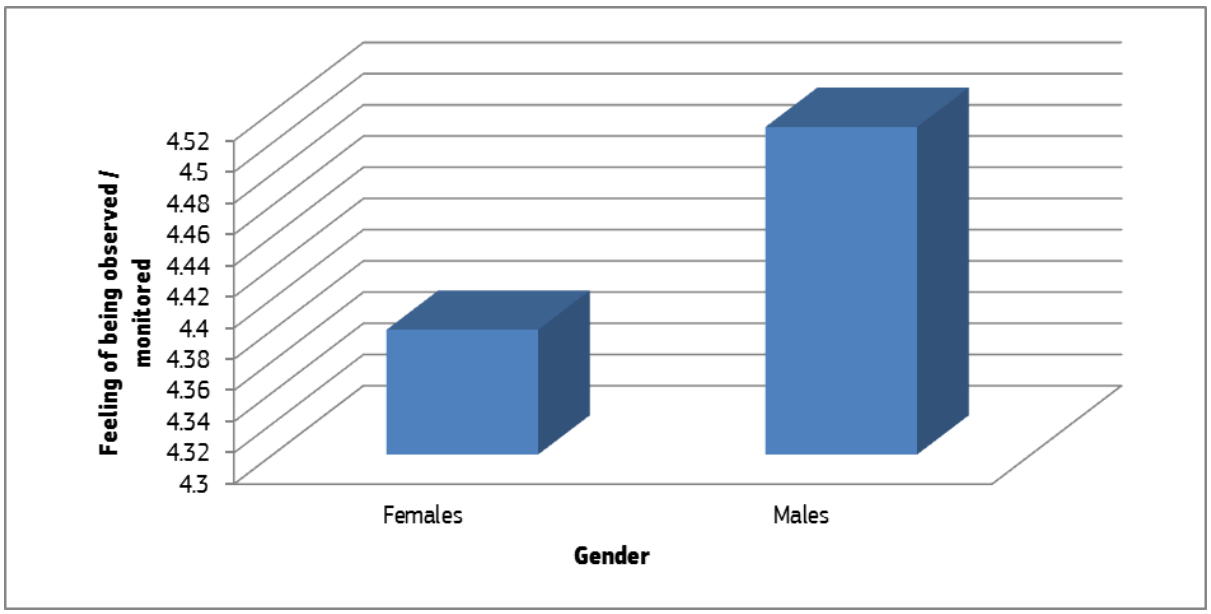
Table 12: Ordered probit regression for the feeling of being observed / monitored with Poland as baseline country

	VARIABLES	Feeling of being observed / monitored
Country	Germany	.309085***
	Italy	-.0842225*
	UK	.0977942*

Gender

The ordered probit regression reveals that females felt significantly less observed than males ($p < 0.01$; Table 10). Their average score in this item was 4.38 (SD = 1.59), compared to 4.51 (SD = 1.49) for males (Figure 13).

Figure 13: Mean feeling of being observed / monitored by gender



Education

Subjects with a higher level of education felt significantly less ($p < 0.01$; Table 10) observed or monitored (M = 4.25, SD = 1.49) than those with a lower level of education (M = 4.66, SD = 1.54; Figure 14).

Age

Younger participants felt significantly less ($p < 0.01$; Table 11) observed or monitored ($M = 4.18$, $SD = 1.54$) than older participants ($M = 4.67$, $SD = 1.47$; Figure 15).

Figure 14: Mean feeling of being observed / monitored by education level

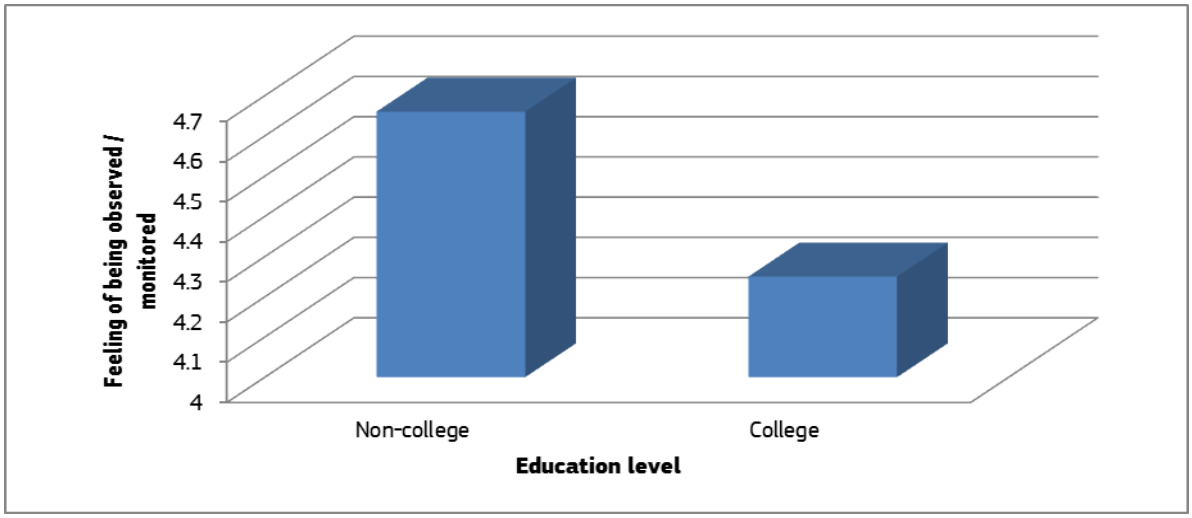
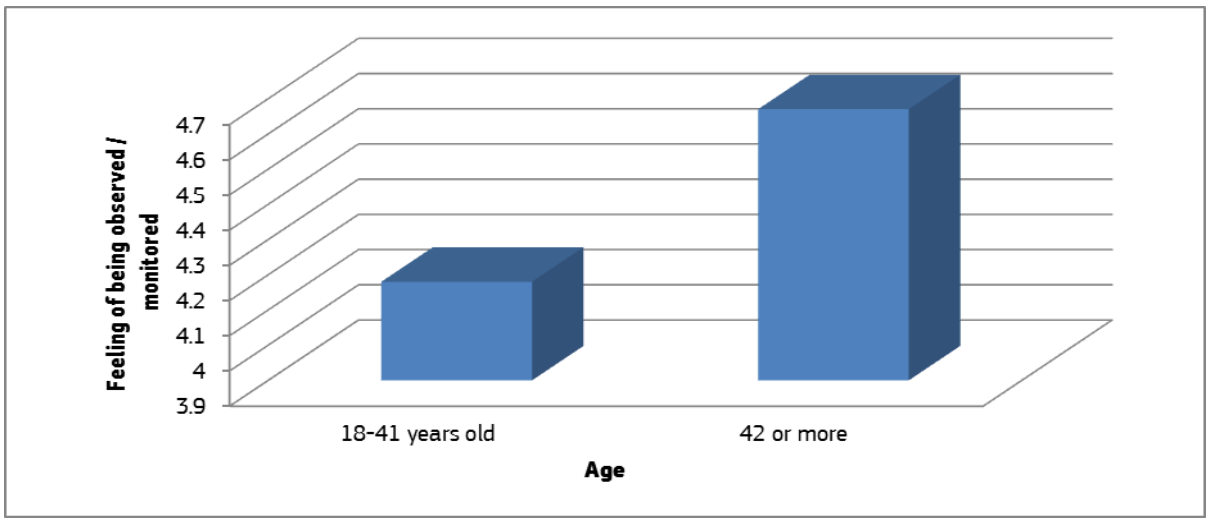


Figure 15: Mean feeling of being observed / monitored by age



Privacy policy link awareness

For this construct, subjects were asked whether they had noticed a privacy policy link in the search engine website with two possible answers ('I noticed it' or 'I didn't notice it'). Differences were tested with a probit model. In this regression, the dependent variable can only take two values and the independent variables are *treatments, country, gender, education level* and *age* (see Table 13).

Treatments

Subjects exposed to the *dynamic anthropomorphic*, *IP address* or *history* treatments were more likely to notice the privacy policy link (Table 13).

Country

Fewer subjects in the UK noticed the privacy policy link during the experiment (92% did not notice the link) compared to the other countries (88% in Germany, 86% in Italy and 87% in Poland; Figure 16).

Table 13: Probit regression for privacy policy link awareness with Control and Italy as baselines for treatment and country

	VARIABLES	Privacy policy link awareness
Treatments	Traditional	.1991768
	Simplified	.1976527
	Anthropomorphic Dynamic	.3314248***
	Anthropomorphic Static	.1674936
	Informal	.0829997
	IP	.2826691**
	History	.3226029***
Country	Germany	-.0755753
	Poland	-.051806
	UK	-.3335011***
Other	Gender	-.1269112***
	Education level	.1117372 ***
	Age	-.102267*

**** p<0.01, ** p<0.05, * p<0.1*

Treatment: Control = 1

Country: Italy = 1; Gender: Female = 1; Education level: College attendants = 1; Age: >42 = 1

Participants in Italy were more likely to notice the privacy policy link than subjects in the UK ($p < 0.01$; Table 13).

If Germany is taken as baseline country, subjects from the UK were less likely to have noticed the privacy policy link, although there were no differences with the other two countries ($p < 0.01$; Table 14).

When Poland is the reference, there are also significant differences showing that subjects from the UK were less likely to see the privacy policy link. No differences were found with the other two countries ($p < 0.01$; Table 15).

Figure 16: Privacy policy link awareness by country in percentage

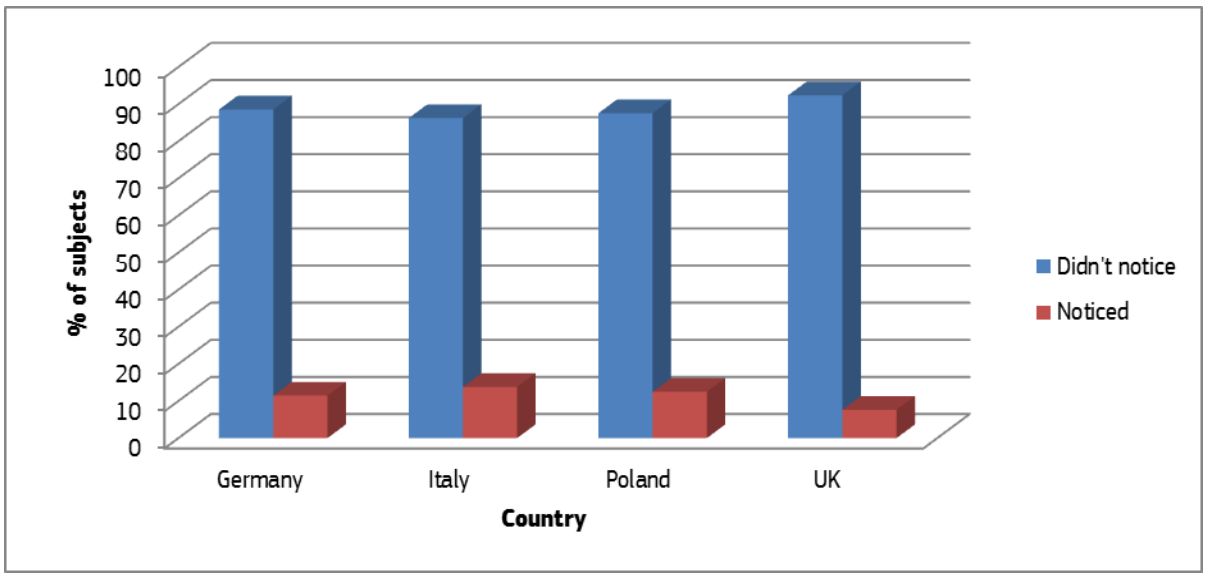


Table 14: Probit regression for privacy policy link awareness with Germany as baseline country

	VARIABLES	Privacy policy link awareness
Country	Italy	.0755753
	Poland	.0237693
	UK	-.2579258***

Table 15: Probit regression for privacy policy link awareness with Poland as baseline country

	VARIABLES	Privacy policy link awareness
Country	Germany	-.0237693
	Italy	.051806
	UK	-.2816951***

Gender

Females were less likely to notice the privacy link than males ($p < 0.01$; Table 14). A lower percentage of women (Figure 17) noticed the privacy policy link (9%) than males (12%).

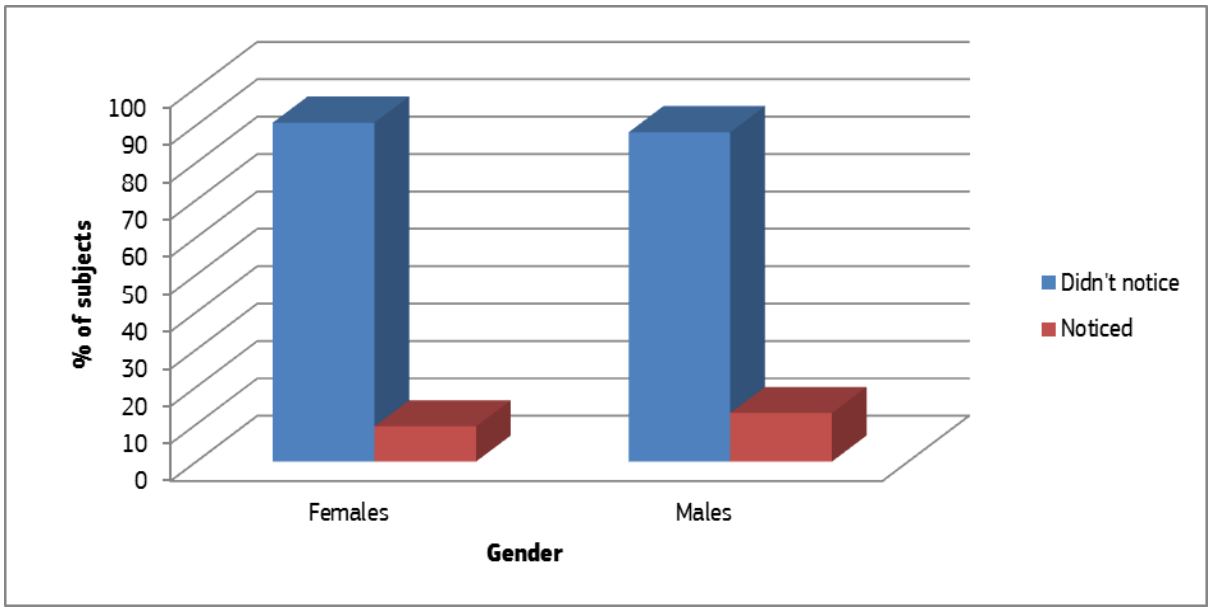
Education

Subjects with a higher level of education were more prone to notice the privacy policy link than those with a lower level of education ($p < 0.01$; Table 13). 54% of subjects who attended college reported noticing the link, compared with 46% of those who never attended college.

Age

Younger participants were more likely to notice the privacy policy link than older ones ($p < 0.10$; Table 14). 54% of younger participants reported noticing the link, compared to 46% of older ones.

Figure 17: Privacy policy link awareness by gender in percentage



V. Discussion and conclusion

This report set out to explore whether changes in the choice architecture of a web interface had an effect on privacy behaviour. It also observed whether less tangible psychological constructs were affected by these changes, and also conducted a demographic analysis according to gender, age, education and country of residence.

Effect of experimental treatments

Results suggest people's disclosure of personal information is not oblivious to changes in the choice architecture. Both dynamic and static anthropomorphic conditions had an effect on passive disclosure. Traditional and dynamic anthropomorphic treatments also had a weak effect on direct disclosure. In both cases, the anthropomorphic characters led people to reveal *more* personal information (not *less*, as suggested by Groom and Calo, 2011). Perhaps this was due to anthropomorphic characters increasing levels of trust and inviting greater disclosure of personal information, as shown elsewhere in the literature (Bente et al., 2014).

However, none of the treatments had an effect on psychological constructs such as the awareness that the answers to the quiz questions revealed personal information, or the feeling of being monitored and the degree of comfort when answering questions. This would seem to confirm that these nudges have an impact on automatic behaviour (the kind Kahneman, 2011, refers to as System 1) rather than behaviour which is guided by in-depth thinking (i.e. System 2). If this is true, they are particularly relevant for habitual and instinctive on-line behaviour.

Changes in the choice architecture did have an effect on whether or not participants noticed the privacy policy link. The presence of an *anthropomorphic character* (the 'dynamic' one), a line showing the participants' *IP address* and a listing of prior browsing *history* all made it more likely that respondents would notice the link. However, noticing the link was not correlated with either *passive* or *direct disclosure*.

Country differences

The study revealed differences in observed behaviour and self-reported answers to a questionnaire according to demographic variables. With regard to country of residence, subjects from Italy revealed the most personal information inadvertently. In addition, they were (a) the least aware that quiz questions revealed personal information about themselves, (b) the ones who felt least observed / most comfortable answering questions, and (c) the ones least likely to disclose personal information directly.

However, the most relevant finding with regard to country differences was that significant country differences existed between *all* countries for direct disclosure (while for passive disclosure only Italy stood out). This would suggest there is an interesting relationship between culture and information disclosure, which merits further investigation.

Gender

With regard to gender, approximately 73% of women answered 'never' to the stigmatized questions, compared to 27% of men. This is a very large difference, and could be because some of the questions (e.g. about alcohol consumption) were less problematic for men to answer. It could also suggest women feel they are under greater social scrutiny, or simply are far more cautious when disclosing personal information. Further qualitative investigation could help to shed light on the causes of this difference.

Neither women nor men were more likely than the other to reveal personal information unwittingly, although women were more aware that the answers to the quiz questions revealed personal information about them. Men, however, felt more observed and less comfortable answering questions than women.

Education

With regard to education, subjects who had attended (though not necessarily graduated from) college felt significantly less observed or monitored and more comfortable answering questions than those who never went to college. This is an odd result, which challenges the assumption that the better educated are more aware of information tracking practices. Further investigation, perhaps of a qualitative nature, could help dig deeper into this issue.

Also, people with a lower level of education were more likely to reveal personal information unwittingly than subjects with a higher level of education. It was also not because they had a greater willingness to reveal personal information, since results for the *direct disclosure* measure show no difference. It is more likely that this is due to the fact that non-college attendees simply were less aware that the answers to the quiz questions revealed personal information about themselves.

Age

Finally, with regard to age, older people (over 41) tended to reveal more personal information inadvertently. There was also a difference in direct disclosure, but in the opposite direction as older individuals revealed less when they were asked directly. No differences were found in the belief that the answers to personal questions revealed information about themselves. However, they did feel more observed / less comfortable when answering questions.

These differences all have potential policy implications. For example, recognising that there are differences in cultural patterns of privacy behaviour could make differentiated implementation of data protection regulation across countries possible. The fact that education plays such an

important role has implications for education policy and the promotion of digital skills. And differences according to age should inform social policy, which aims to ensure no generation is left behind in the information society.

A final word…

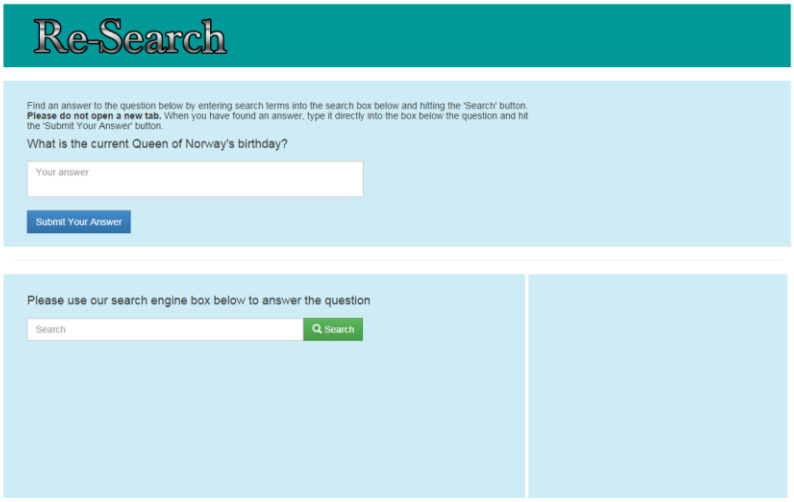
By conducting an experiment on privacy nudges, this report has attempted to bring behavioural research methods for privacy to the attention of European policy-makers. It has considered the opportunities and challenges of applying behavioural insights to privacy legal frameworks. However, this study has its limits. It has only targeted a sample of users in four countries in an experimental setting (even though every effort was made to ensure that the experiment was as realistic as possible). The question still remains: how would hundreds of thousands of people react to these changes in a real-life setting?

The major web service providers (e.g. Google, Facebook, Twitter) are likely to have extensive amounts of data on how slight changes to their services' privacy controls affect users' privacy behaviour. One policy recommendation, therefore, is that national and European privacy enforcement authorities should work with these providers to leverage this data to inform appropriate privacy and data protection rules, regulations, laws, and legislation. These service providers should not be forced to hand over this data; rather, they could work together, in partnership, to arrive at recommendations for web interface design that allow for an aware disclosure of privacy information.

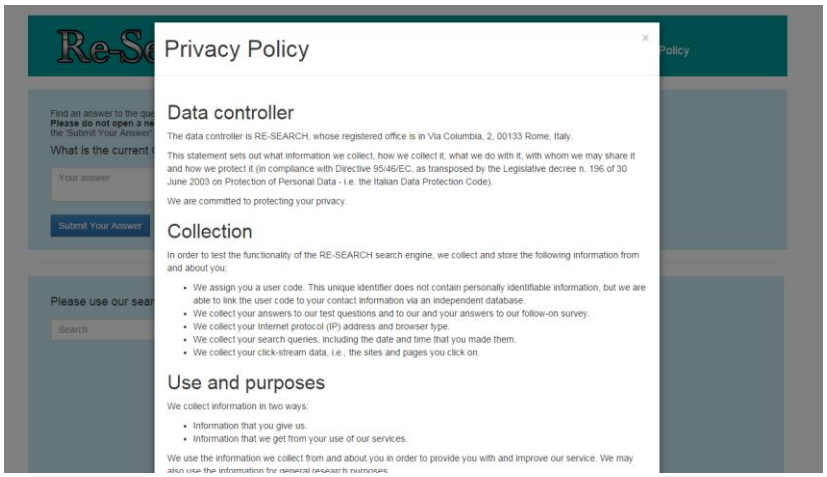
Annex 1

Screenshots of the experimental conditions

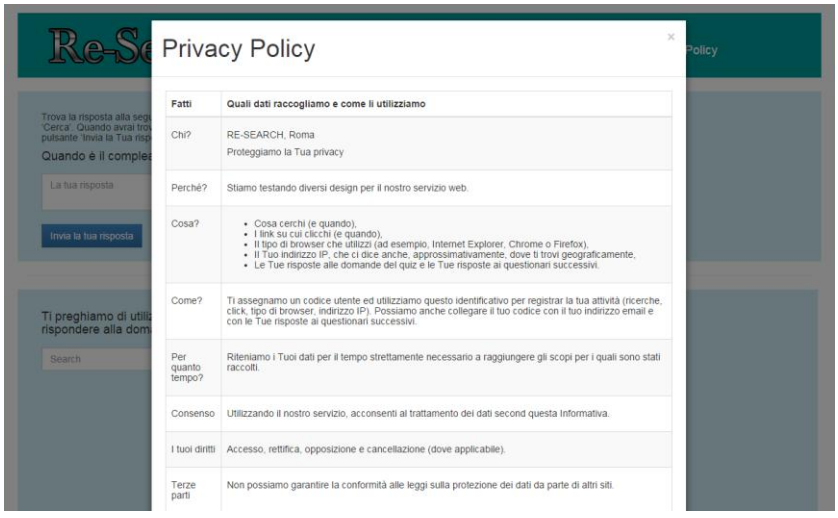
1. Control



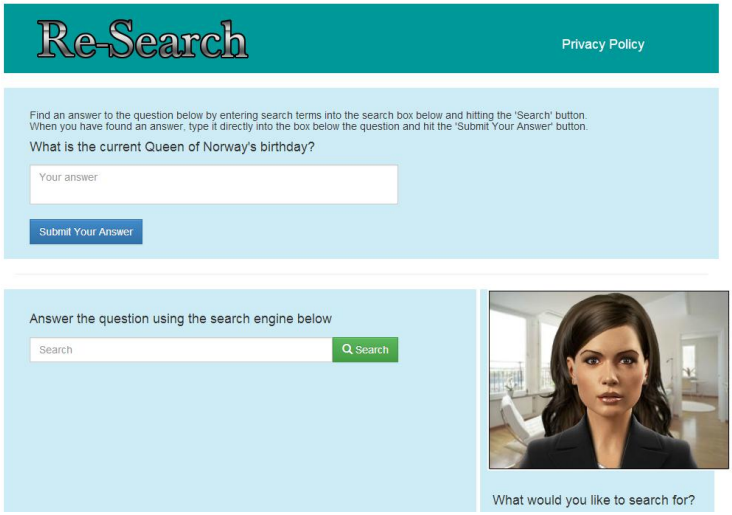
2. Traditional



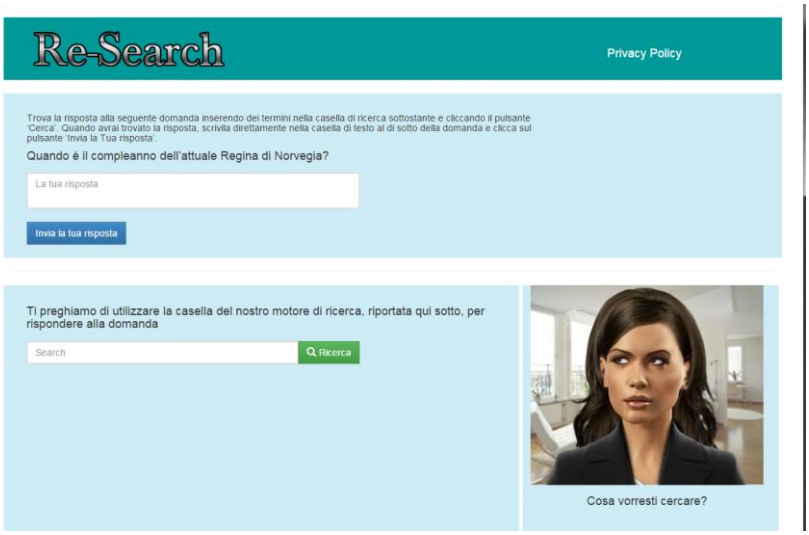
3. Simplified



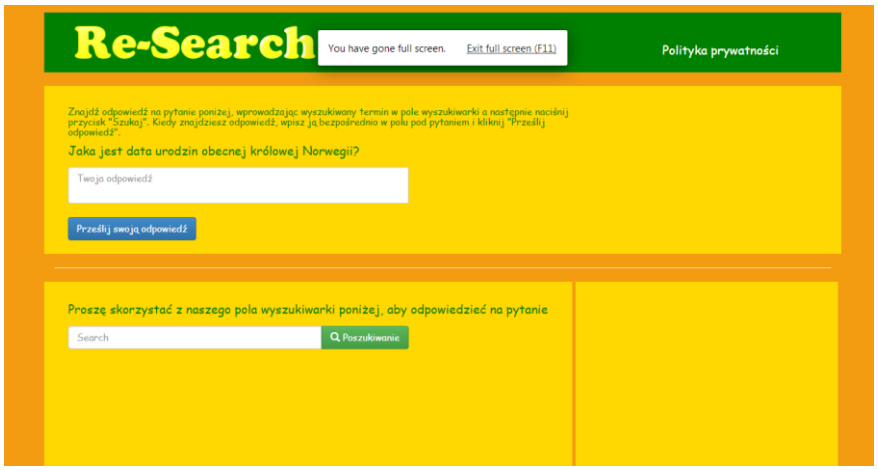
4. Static agent



5. Interactive agent

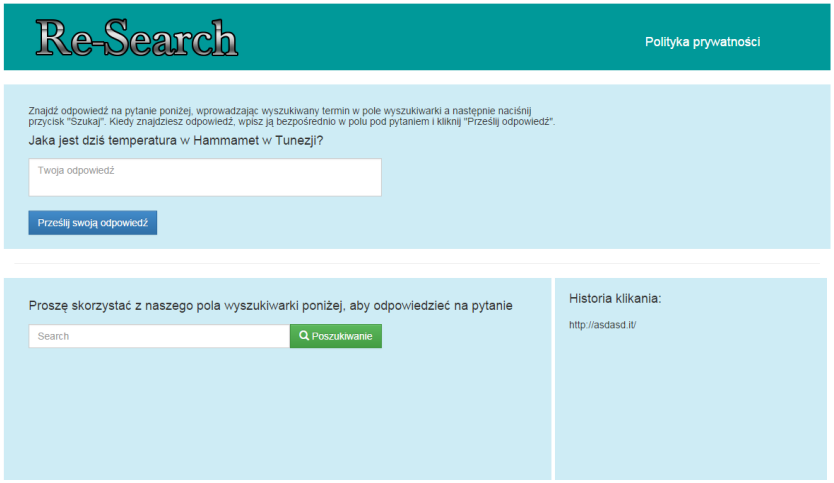


6. Informality



7. IP information

8. History



Annex 2

Questionnaire

I. Trivia Questions

1. What is the current Queen of Norway's birthday?
2. What is the high temperature today in Hammamet, Tunisia?
3. What is the name of the national opera house in Kiev?
4. Who is the current European Commissioner for Development?

II. Passive Disclosure

Sensitive Questions in *Italics*

Set 1:

5. Find a recipe for chocolate cake and list all the ingredients
6. Provide the name of the winner at the Eurovision song contest in 1978
7. *Provide the name of a famous public figure or celebrity born the same year as you*

Set 2:

8. *What is the street address of a post office in the town where you live?*
9. What is the date of the first full moon in the year 2017?
10. On what date was the highest temperature in the U.S.A. recorded?

Set 3:

11. *In what year was the bank you use founded?*
12. Which years marked the beginning and the end of the Crimean War?
13. Which Shakespeare play was first performed in 1604?

Set 4:

14. What are the names of three of the moons of Neptune?
15. What is the full name of the 81st element in the periodic table?
16. *What is the address of your favourite restaurant located in the town where you were born?*

III. Internet usage

17. What browser do you typically use?
18. What operating system do you typically use?
19. What search engine do you typically use?
20. Are you a member of a social networking site, such as Facebook?

IV. Search engine

21. Do you think the search engine you tested is easier to use than the search engine that you typically use?
22. Do you think the search engine you tested is more efficient in the result provided than the search engine that you typically use?
23. Do you think the search engine you tested fits your needs better than the search engine that you typically use?

V. Direct Disclosure

24. Have you ever claimed to have education that you didn't actually have?
25. Have you ever pretended not to see a beggar to avoid being seen as stingy?
26. Have you ever had sex with someone who was too drunk to know what they were doing?
27. Have you ever looked at pornographic material?
28. Have you ever had sex with the current husband, wife, or partner of a friend?
29. Have you ever known about or witnessed a serious crime and failed to report it or stop it?
30. Have you ever lied about your income to someone?
31. Have you ever fantasized about having violent non-consensual sex with someone?
32. Have you ever drunk so much that you got a hangover?
33. Have you ever failed to tip a waiter in a country in which tipping is customary?

VI. Answers provided

34. My answers to the quiz questions revealed personal information about myself
35. I felt comfortable answering personal questions during this study
36. I felt observed during this study
37. I felt I was being monitored during this study

VII. Personal information captured

38. The search engine website was able to detect several pieces of information about my online activity
39. The websites you visited
40. The web browser you used
41. The search terms you used
42. Your Internet Protocol (IP) address
43. Your geographic location
44. Your answers to the questions about web use
45. The time you started the quiz questions
46. The time it took for you to complete the quiz questions
47. The year of your birth
48. The town you are currently connected from

VIII. Noticing elements

49. While you were answering the quiz questions, did you notice anything unusual in the right side of the screen? Please describe what you noticed, if anything
50. While you were answering the quiz questions, did you notice a link to a privacy policy for the search engine?
51. While you were answering the quiz questions, did you notice a series of links to URLs you had visited?
52. While you were answering the quiz questions, did you notice an IP address?
53. While you were answering the quiz questions, did you notice a geographical location? Was it the correct location from which you are currently connected?

54. While you were answering the quiz questions, did you notice a browser name? Was it the correct name of the browser you are currently using?
55. While you were answering the quiz questions, did you notice an image of a female character?

IX. **Socio-demographics**

56. You are:
57. How old are you?
58. Your education level:
59. Your employment situation:
60. Your personal income (net monthly salary) is:
61. How many people live in your household, including you?
62. Your household average income (net monthly salary) is
63. For which political party did you vote at the last elections?

X. Other

64. Did you complete this study alone or with others?
65. Where did you connect from?
66. What device did you use to take this survey?
67. What was the goal of this study?
68. Do you have any comment or suggestion for this study?

Annex 3

Sample characteristics and socio-demographics

The distribution of the sample corresponded to 49% of females (Table A – Figure A). Participants were divided into groups of 7 years of range (e.g. 18-25, 26-33, etc.), though they were afterwards merged into two categories due to differences in the results of the statistical analysis conducted. The first group included participants between 18 and 41 vs. subjects over 42 years old, distributed as shown in Table B – Figure B. Participants were also allocated according to their education level depending on whether they had attended to college or not (Table C – Figure C).

Table A: Participants' distribution by gender

Country	Gender	Frequency	% Country	% Sample
Germany	Female	398	48.95	12.34
	Male	404	49.69	12.52
	I prefer not to answer	11	1.35	0.34
Italy	Female	374	46.93	11.59
	Male	408	51.19	12.65
	I prefer not to answer	15	1.88	0.46
Poland	Female	394	49.13	12.21
	Male	401	50.00	12.43
	I prefer not to answer	7	0.87	0.22
UK	Female	402	49.39	12.46
	Male	405	49.75	12.55
	I prefer not to answer	7	0.86	0.22
Total		3,226		100.00

Figure A: Gender distribution of the total sample

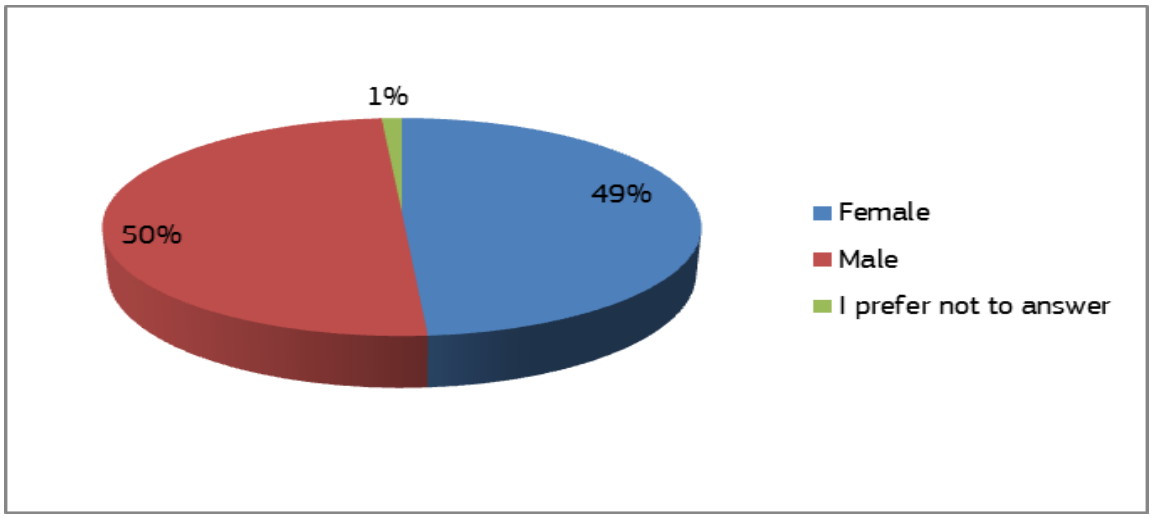
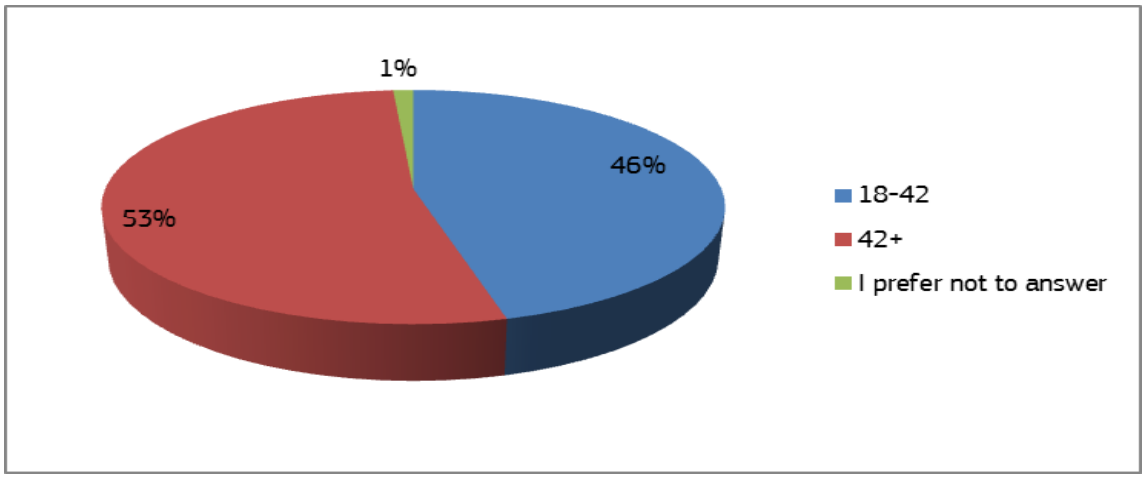


Table B: Participants' distribution by age

Country	Age	Frequency	% Country	% Sample
Germany	18-41	332	40.84	10.29
	42 and above	472	58.06	14.63
	I prefer not to answer	9	1.11	0.28
Italy	18-41	439	55.08	13.61
	42 and above	346	43.41	10.73
	I prefer not to answer	12	1.51	0.37
Poland	18-41	433	53.99	13.42
	42 and above	361	45.01	11.19
	I prefer not to answer	8	1.00	0.25
UK	18-41	275	33.78	8.52
	42 and above	529	64.99	16.40
	I prefer not to answer	10	1.23	0.31
Total		3,226		100.00

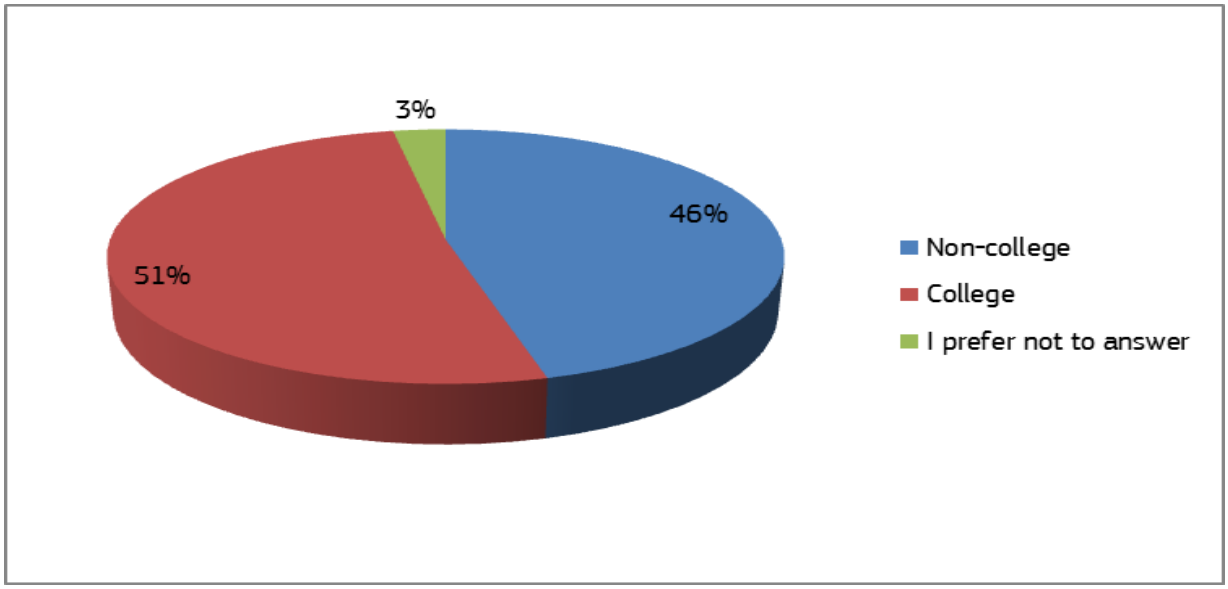
Figure B: Age distribution of the total sample



Participants' distribution by level of education

Country	Gender	Frequency	% Country	% Sample
Germany	Non-college	503	61.87	15.59
	College	271	33.33	8.40
	I prefer not to answer	39	4.80	1.21
Italy	Non-college	357	44.79	11.07
	College	424	53.20	13.14
	I prefer not to answer	16	2.01	0.50
Poland	Non-college	354	44.14	10.97
	College	430	53.62	13.33
	I prefer not to answer	18	2.24	0.56
UK	Non-college	262	32.19	8.12
	College	533	65.48	16.52
	I prefer not to answer	19	2.33	0.59
Total		3,226		100.00

Figure C: Education level distribution of the total sample



References

Acquisti, A. (2009). Nudging privacy: Behavioral economics of personal information. *Security & Privacy*, 7(6). 82–85.

Acquisti, A. (2010a). From the economics to the behavioral economics of privacy: A note. *in Ethics and Policy of Biometrics, 6005 Springer*.

Acquisti, A. (2010b). The economics of personal data and the economics of privacy. Background paper for the *Joint WPISP-WPIE Roundtable The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines*. OECD.

Acquisti, A. & Grossklags, J. (2007). What can behaviorual economics teach us about privacy? In Acquisti, A., Gritzalis, S., Lambrinoudakis, C., and di Vimercati, S. (Eds.). *Digital Privacy: Theory, technologies, and practices*. CRC Press.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. J*ournal of Marketing Research*, 49(2), 160-174.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Bente, G., Dratsch, T., Rehbach, S., Reyl, M., & Lushaj, B. (2014). Do you trust my avatar? Effects of photo-realistic seller avatars and reputation scores on trust in online transactions. In *HCI in Business* (pp. 461-470). Springer International Publishing.

Borgesius, F. (2013). Consent to behavioural targeting in European law: What are the policy implications of insights from behavioural economics? *Conference paper for Privacy Law Scholars Conference (PLSC), 6-7 June 2013, Berkeley,US*.

Calo, R. (2012). Against Notice Skepticism in privacy and elsewhere. *Notre Dame Law Review. vol. 87*.

Calo, R. (2014). Code, Nudge or Notice? *Iowa Law Review, vol. 99, no. 2 ; University of Washington School of Law Research Paper No. 2013-04. Available at SSRN: http://ssrn.com/abstract=2217013*, 773-802.

Cavoukian, A. (2012). Privacy by design and the emerging personal data ecosystem. *Privacy By Design*.

European Commission (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM(2012) 11 final.

Groom, V., & Calo, M. R. (2011). Reversing the privacy paradox: An experimental study. *TPRC Conference proceedings, available at SSRN: http://ssrn.com/abstract=1993125*.

Haynes, A. (2007). Online privacy policies: Contracting away control over personal information? *Penn State Law Review Vol 111: 3*, 587-624.

Hildebrandt. (2012). The Dawn of a Critical Transparency Right for the Profiling Era. In M. C. Ed. J. Bus, *Digital Enlightenment Yearbook 2012* . IOS Press, Amsterdam.

Hinton, P. R., Brownlow, C., McMurray, I. & Cozens, B. (2004). *SPSS explained*. Routledge, East Sussex, UK.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? Available at SSRN: http://ssrn.com/abstract=1589864 or HYPERLINK "http://dx.doi.org/10.2139/ssrn.1589864"

Hoofnagle, C.J. & King, J. (2008). What Californians understand about privacy online. Available at SSRN 1262130.

John, L., Acquisti, A., & Loewenstein, G. (2009). The Best of Strangers: Context Dependent Willingness to Divulge Personal Information. *Available at SSRN: http://ssrn.com/abstract=1430482 or http://dx.doi.org/10.2139/ssrn.14*.

Kahneman, D. (2011). *Thinking, fast and slow.* Penguin.

Lunn, P. (2014). *Regulatory Policy and Behavioural Economics*, OECD Publishing.

Lusoli, W., Bacigalupo, M., Lupiáñez-Villanueva, F., de Andrade, N.N.G., Monteleone, S. & Maghiros, I. (2012). Pan-European survey of practices, attitudes and policy preferences as regards personal identity data management. *JRC Scientific and Policy Reports*, EUR 25295. Luxemburg: Luxemburg Publications Office.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. *Pew Research Center*, *21*. Available at http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

Martin, K.E. (2013). Transaction costs, privacy and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday Vol. 18, 12*.

McDonald, A., & Cranor, L. (2008). Cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society, 4:*543.

Shafir, E. (2013). *The Behavioral Foundations of Public Policy*. Princeton University Press.

Solove, D. (2013). Introduction: Privacy self-management and the consent dilemma. *126 Harvard Law Review*, 1880.

Solove, D. & Hoofnagle, C. (2006). A model regime of privacy protection (Version 3.0). *University of Illinois Law Review, Vol. 2006, No. 2*.

Sunstein, C.R. (2000). *Behavioural Law and Economics.* Cambridge University Press.

Sunstein, C.R. (2013). Behavioral economics, consumption, and environmental protection. *Regulatory Policy Program Working Paper RPP-2013-19. Cambridge, MA: Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, Harvard University*.

Thaler, R., & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth, and happiness.* Yale University Press.

Tsai, J., Cranor, L., Acquisti, A., & Fong, C. (2006). What's it to you? A survey of online privacy concerns and risks,. *Preliminary Progress Report NET Institute Working Papers n. 06-29*.

van Bavel, R., Herrmann, B., Esposito, G., & Proestakis, A. (2013). *Applying Behavioural sciences to EU policy-making, JRC Scientific and Policy Reports EUR 26033 EN* . http://ec.europa.eu/dgs/health_consumer/information_sources/docs/30092013_jrc_scientific_policy_report_en.pdf.

Wang, Y., Leon, P., Scott, K., Chen, X., Acquisti, A., & Cranor, L. (2013). Privacy nudges for social media: an exploratory Facebook study. *Proceedings of the 22nd international conference WWW '13 Companion*.

World Bank (2015). *World Development Report 2015: Mind, Society, and Behaviour* (http://www.worldbank.org/en/publication/wdr2015).

Wu, K., Huang, S.Y., Yen, D., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior (28)*.

European Commission
EUR 27384 EN – Joint Research Centre – Institute for Prospective Technological Studies

Title: Nudges to Privacy Behaviour: Exploring an Alternative Approaches to Privacy Notices

Authors: Shara Monteleone, René van Bavel, Nuria Rodríguez-Priego, Gabriele Esposito

Luxembourg: Publications Office of the European Union
2015 – 42 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online)
ISBN 978-92-79-50320-7 (PDF)
doi:10.2791/142795

LF-NA-27384-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2791/142795

ISBN 978-92-79-50320-7

Publications Office