Awareness, values and attitudes of user generated content website users and non-users towards privacy in Europe: a qualitative study

Noellie Brockdorff[1], Sandra Appleby-Arnold[1], Bogdan Manolea[2], Ioana Vasiu[3]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Association for Technology and Internet, Bucharest, Romania
[3] Faculty of Law, Babeş-Bolyai University, Cluj-Napoca, Romania

April 2013

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

CONSENT
Consumer Sentiment regarding privacy on user generated content (UGC) services in the digital economy (G.A. 244643).
The project was co-financed by the European Union within the Seventh Framework Programme (2007-2013).
http://www.consent.law.muni.cz

Correspondence about this report should be addressed to
Noellie Brockdorff, Department of Cognitive Science, University of Malta, Msida, MSD2080, Malta
noellie.brockdorff@um.edu.mt

Table of Contents

1. Key Findings

The following are the key findings of a study undertaken as part of the CONSENT project (work package 8). It consisted of a set of 131 semi-structured in-depth interviews regarding the values and attitudes of user generated content (UGC) website users towards privacy. A quota sample of UGC users and non-users (20%) was used which aimed at achieving as wide and even a representation as possible in terms of gender, age and location. The interviews were conducted between May and July 2012 in the following partner countries: Bulgaria, Czech Republic, Denmark, France, Germany, Italy, Malta, the Netherlands, Poland, Romania, Slovakia, Spain, and the United Kingdom.

1. Interviewees were typically very frequent, experienced and avid internet users who see a number of advantages in using the internet, in particular the availability of, and speed of access to, information. At the same time, they had a rather critical attitude towards the internet in general, showing also concern regarding a lack of privacy and absence of control over personal data.
2. Most UGC users experienced an internal conflict between wishing to keep control of their personal data and a perceived need, or desire, to use UGC services. A number of different strategies were used for dealing with this conflict.
3. Interviewees in most countries were less willing to give personal information online than in offline situations. A majority outlined their uncertainty about what is happening to their personal data online and who is holding it and possibly sharing it with unknown others.
4. Being engaged in UGC usage did not necessarily go alongside a greater willingness to disclose information for commercial trade-offs, and being open to commercial trade-offs was not linked to a more "generous" disclosure of personal and private information on UGC sites.
5. There was a considerable disparity between reaction to some common website practices, such as the customization of content and advertising, which is largely accepted, and practices that are less well known such as the sharing or selling of UGC users' personal information which were generally deemed unacceptable.
6. The customization of content and advertising seen by users was accepted by the majority of interviewees in most countries as a commercial trade-off, the "the price to pay" for a free service, or considered as "normal" or "inevitable". However, in Denmark and the UK the majority of interviewees did not accept this practice and felt that it represented an interference in their private life, infringing on their privacy, and linked it to the idea of surveillance.
7. The website owners' practice of sharing and selling personal user information to third parties was mostly deemed unacceptable due to a fear of losing control both at the point of first information disclosure and when using the website, but also through the uncontrollable use by third parties at any future point in time. This practice also went counter to the strong desire on the part of interviewees to be able to decide themselves which data would be shared or sold, when and to whom – even in the case of anonymized data. Rejection of this practice may also be linked with unease that users' perceptions of privacy may differ from those of website owners.

8. The most common measures taken to protect privacy online practice was to exercise caution in disclosing personal or private information online. More proactive measures varied according to the interviewees' levels of awareness and experience of possible data misuse, knowledge of the possibilities and limitations of changing privacy settings and the technical ability to do so.
9. The majority of interviewees in most countries stated that they usually do not read privacy policies. Reasons for not reading privacy policies can be divided into two categories: technical and content. At a technical level, privacy policies were not read because they are too long, written in text that is too small and too difficult to understand. On the level of content, interviewees did not feel the need to read privacy policies because they are "always the same", or because the contents would already be familiar due to discussions in the media.
10. Those who did read privacy policies viewed this as part of a learning process that is indispensable if one wishes to assume responsibility for one's personal information and be able to take adequate protective measures.
11. A common perception amongst both readers and non-readers of privacy policies was that privacy policies primarily serve the purpose of protecting the website owners rather than the website users.
12. Two distinct perceptions relating to the control of personal data online are evident: either generally elevated levels of perceived control or perceived lack of control over one's personal information.
13. Elevated levels of perceived control were linked to a limited experience of online privacy violation, the belief that the existing legal data protection framework provides sufficient protection or the extension online of the prevailing offline conditions of perceived social order and protection by law.
14. Perceived lack of control was linked to either the concept of privacy being underdeveloped, or a perceived helplessness which was often masked as disinterest in online privacy issues.
15. Users who have overcome inertia and accepted personal responsibility for their online privacy appeared to accept that in the online environment there is no ultimate guarantee for privacy protection, and that there remains an inherent uncertainty which cannot be resolved.

Country Highlights

The following are findings that were particularly prevalent in individual countries, although they may also hold for subgroups of internet users with similar profiles elsewhere. The findings below also represent those areas in which findings in particular countries differed from findings overall. These results are not described in this report but are discussed in full in the relevant individual country reports produced as part of this study.

16. **Bulgaria, Romania Slovakia** The concept of privacy appeared to be much less developed than elsewhere. Lack of control of personal data online was, partially, denied and masked as disinterest. At the same time, lack of experience in internet use and perceived helplessness to successfully enforce user interests seem to mutually reinforce each other, resulting in what may superficially appear as user inertia.

17. **Czech Republic, Poland** Much less concern about online privacy than generally the case in other countries. This may be the product of limited experience of negative outcomes resulting from misuse of personal data online and privacy violations associated with such misuse. In Poland, it was paired with a strong tendency to assume personal responsibility for managing disclosure of personal data online.
18. **Denmark** Online privacy was felt as being "guaranteed", through the extension of the prevailing "offline" conditions of perceived social order and protection by law, and the application of common values (such as solidarity between citizens) and common sense. However, there were undertones of increasing insecurity and self-confidence being shaken in relation to online privacy.
19. **France** Privacy was perceived as something that is struggled with and fought for between the rights and obligations of "digital citizenship". There is acceptance of the commercial needs of website owners but also a feeling that there is a lack of power balance between website owners and users
20. **Germany** There are generally elevated levels of perceived control of personal data disclosed online apparently linked to the belief that the existing legal data protection framework provides sufficient protection. However, there was also some awareness that this may be an "illusion of control".
21. **Italy, Malta** Uncertainty in online privacy and that online there is no "hard" boundary between what is public and what is private were seen as facts of life. However, online privacy is seen as a desirable social value. Managing one's online privacy is considered a matter of personal responsibility. Attitudes towards the use of personal information disclosed online by website owners oscillated between dislike, the perceived need to monitor these practices, accepting them as a commercial trade-off, and appreciating potentially positive effects.
22. **Netherlands** UGC users attempted to reduce the uncertainty associated with online privacy through gathering of other people's experiences and opinions regarding the usage of specific UGC websites. These shared experiences and public opinion in general were important in this situation. Such attempts at reducing uncertainty could result in increased feelings of security or insecurity, depending on the information received.
23. **Spain** There was awareness that online privacy may not be secure but, at the same time, there were also perceptions of security by merging offline intimacy with online privacy, transferring established social values such as "family" as a protected space into the online context.
24. **United Kingdom** Users had a strong reliance on their generally extensive internet experience and high level of technical protection skills for the purposes of managing online privacy, but paired with low levels of awareness of the use by website owners of personal information disclosed by users on UGC websites. Once website owners' practices relating to the use of personal information became known they caused a high level of frustration and anger as well as disapproval of these practices.

2. Introduction

2.1 Study

The analyses and results in this document are based on a set of semi-structured in-depth interviews regarding the values and attitudes of user generated content (UGC) website users towards privacy. This study was undertaken as part of the CONSENT[1] project.

This document synthesises the findings from all participating countries. Separate country-specific reports are available for Bulgaria, Czech Republic, Denmark, France, Germany, Italy, Malta, the Netherlands, Poland, Romania, Slovakia, Spain, and the United Kingdom.

The interview guideline used in this study consisted of 27 questions and sub-questions covering general internet usage and perceptions relating to internet use, and individual attitudes and behaviour regarding the use of UGC websites probing in particular those related to the disclosure of personal and private information. The interview also investigated attitudes towards the use of this personal user information by website owners for various commercial purposes, the consequences of these commercial practices for users, and the strategies employed by UGC users and UGC non-users to deal with the need to disclose personal information online when using websites.

[1] "Consumer Sentiment regarding privacy on user generated content (UGC) services in the digital economy" (CONSENT; G.A. 244643) – which was co-financed by the European Union under the Seventh Framework Programme for Research and Technological Development (SSH-2009-3.2.1. "Changes in Consumption and Consumer Markets").

2.2 Methodology

The analysis in this report is based on 131 interviews – ten in each of the abovementioned countries[2] – which were conducted between May and July 2012. Personal references and snowball techniques were used to find individuals willing to take part in this study which, as a qualitative analysis, does not claim to be representative for an entire EU population or any of the individual EU countries where interviews were conducted. However, in order to ensure adequate representation of different sub-groups participating partner countries were required to select interviewees following certain quota as shown in the table below.

Total Number of Interviews = 10 per country			
UGC users		8	4 male / 4 female, of which at least 6 use SNS (at least 1 male and 1 female), and 2 (1 male and 1 female) that use UGC, but not SNS.
UGC non-users		2	1 male / 1 female
Gender	**Male**	5	
	Female	5	
Location	**Urban/ suburban**	8	4 male / 4 female
	Rural	2	1 male / 1 female
Age group	**15-24**	3	
	25-34	3	of which 1 UGC non-user
	35-44	2	
	45+	2	of which 1 UGC non-user

The breakdown of interviewees' characteristics comprised, as a basic categorisation, an even gender distribution and an 8:2 split between UGC users and non-users, with the UGC users preferably including two interviewees who were not users of Social Networking Sites (SNS). Then, the interview requirements were split further down by location and age group, aiming at as wide a representation as possible whilst keeping the total number of interviews per CONSENT partner at a manageable level.

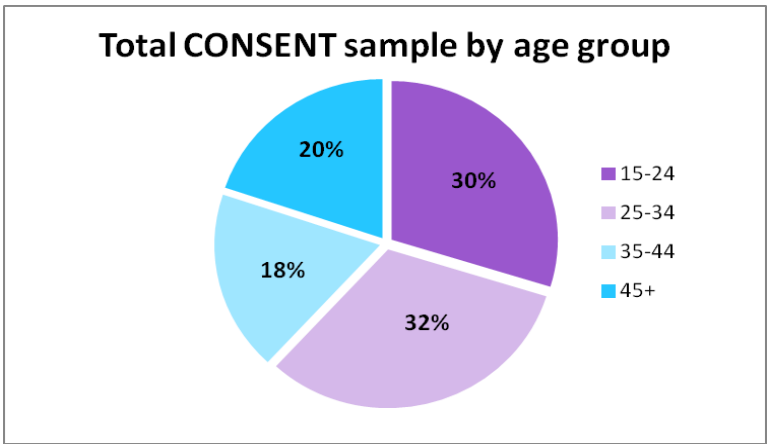
Interviews were carried out in the national language following an interview guideline that was also translated to local languages (see Appendix A for English version of interview guideline). After the interviews were conducted they were fully transcribed in the local language, and a pre-analysis template for each interview was filled out in English. The development of this template was based on pilot interviews conducted earlier, and it served primarily for the collating, formal structuring and pre-coding of the vast amount of collected data. Then, the content of each set of country templates was analysed section by section, labelling them with additional codes which either summarised specific processes and practices or constructions and interpretations[3]. This process of re-coding also initialised a critical restructuring and rethinking of the codes applied initially, and allowed for a more focussed data analysis and drawing together of overarching themes. Finally, a draft version of each country report was submitted to the respective partner for revision and amendments.

[2] In Germany the analysis is based on 11 interviews.

[3] Data could fall into different categories at the same time and were then also double-coded as such.

2.3 Sample

The data analysis is based on 131 interviews with a demographic distribution as shown in the graph and tables below:



Age Group	Male		Female		Total	
	Count	%	Count	%	Count	%
15-24	21	54%	18	46%	39	100%
25-34	28	67%	14	33%	42	100%
35-44	7	29%	17	71%	24	100%
45+	12	46%	14	54%	26	100%
Total	68	52%	63	48%	131	100%

Overall a fairly even split between male (52%) and female (48%) interviewees was achieved, although there is a certain over-representation of male interviewees in the 25-44 age group, and of female interviewees in the 35-44 age group.

Age Group	UGC user		UGC (non-SNS) user		UGC non-user		Total	
	Count	%	Count	%	Count	%	Count	%
15-24	35	90%	3	8%	1	3%	39	100%
25-34	23	55%	9	21%	10	24%	42	100%
35-44	19	79%	2	8%	3	13%	24	100%
45+	10	38%	5	19%	11	42%	26	100%
Total	87	66%	19	15%	25	19%	131	100%

Regarding the distribution of UGC usage and non-usage, the desired gender quota was mostly achieved both within the group of UGC users (43 male / 45 female) as well as within the group of UGC non-users (10 male / 14 female). Within the group of UGC (non-SNS) users a slightly higher representation of female interviewees (6 female / 13 male) would have been desirable. Regarding UGC usage within the different age groups the desired quota was achieved. The same applies to location, where male and female respondents were evenly represented (urban/suburban location: 52 male, 49 female; rural location: 15 male, 13 female). In terms of interviewees' level of internet experience, the majority of interviewees had been using the internet for at least ten years. Examining the relation between SNS usage and the age when these respondents started to use the internet, there was no recognisable link between being a "digital native" or a "digital initiate" and using, or not using, SNS websites.

3. Results

3.1 Attitudes to User Generated Content websites

On the one hand, the vast majority of interviewees appeared to be very frequent, experienced and avid internet users who clearly perceived a number of advantages to using the internet, in particular the availability of, and speed of access to, information. On the other hand, many interviewees expressed a rather critical attitude towards the internet in general – particularly regarding the lack of privacy and absence of control over personal data.

This critical attitude to the internet was equally prevalent amongst interviewed UGC users and non-users. It seems that the non-usage of UGC websites was not related to privacy concerns, rather it was due to UGC websites being perceived as not useful or not interesting to non-users.

Only in a few cases (in Spain and in France) were privacy concerns given as the predominant reason for not using UGC websites or Social Networking Sites. In Bulgaria, Romania and Slovakia, privacy concerns generally were expressed very vaguely and this was also the case during the discussion of reasons for not using UGC websites. In these three countries UGC non-users (or low-frequency users) referred to themselves as "pragmatic" users, constructing a "non-relationship" in which an active engagement and serious examination of possible risks was perceived as unnecessary.

Most interviewed UGC users exhibited a form of tension between wishing to keep control and a perceived need, or desire, to use UGC services. These interviewees revealed a number of different strategies for dealing with this tension:

- in a playful manner, e.g. by intentionally merging real-world and fake identities (e.g. in Italy);
- by critical self-reflection about their "illusion of control" (e.g. in Germany);
- by thinking of themselves as "pragmatic" or "utilitarian" users (e.g. in Romania, Slovakia; see also above regarding non-users);
- by rationalisation through the transferring of offline social norms, such as the trust in family and friends, to the online context (e.g. in Malta, Spain);
- by depending on some form of "public social control" and common sense, exercised by the mass media and the mass of users itself (e.g. in Denmark, UK);
- by thinking of risks in general as "insurable" (similar to home or life insurances) through the existing offline social order and, thus, controllable (e.g. in Denmark); or
- by depending on the value they assign to online privacy being shared by other users.

3.2 Information Disclosure – "Offline" and Online

The relationship between the online behaviour of UGC users and non-users and their attitudes and perceptions "offline" in relation to privacy-related social norms was investigated through the use of a number of scenarios. Respondents were encouraged to imagine a situation where, whilst travelling on a plane, a stranger would ask them a number of personal questions, and whether they would reveal their marital status, their income, and their ID card or passport number to this stranger. After that, they were requested to talk about their reaction if the same questions were asked by a friend.

In these imagined "offline" situations, it strongly depended on the type of personal or private information[4] whether or not the interviewees would disclose it.
Independent from age, gender, UGC (non-)usage or national background, most interviewees revealed very similar attitudes towards the disclosure of such information to strangers or friends "offline". Interviewees generally differentiated between the three classes of personal and private information listed below.

(a) Information that is perceived as personal but not very private (marital status) and, thus, would mostly be disclosed to friends as well as to strangers.
(b) Information that is perceived as private with its privacy status being a social norm (income). In this case some interviewees imagined their reaction to go beyond simply either disclosing or not disclosing the information requested. The "offline" situation allowed them to counteract, negotiate and establish or re-establish perceived social norms and boundaries – not only with friends but also with strangers.
(c) Information which was considered private and critical (ID card or passport number), disclosure of which was associated with potential personal risks, in particular fraud and identity theft.

Whereas the interviewees' responses revealed a comparably homogeneous pattern of answering in offline situations with both strangers and friends, there was a wider variation in answers regarding what information would be disclosed online in the context of online shopping / commercial trade-offs, and even more so on UGC websites.[5] Here, reasons for non-disclosure were linked to information that could be divided into different, though partially overlapping, categories:
(a) Information requested perceived as "too private";
(b) The disclosure of the requested information was linked to the perceived risk of fraud;
(c) The disclosure of the requested information was linked to the perceived risk of receiving unwanted commercial offers;

[4] The distinction made here between "personal" and "private" is following educational definitions where personal information cannot be used to identify someone (in the sense of identity theft), whereas private information can be used to identify someone and may be unsafe to share. This distinction is currently not being made in data protection law which only refers to "personal" data/information, in common language both terms are often used synonymously, within the various scientific disciplines there is a wealth of different definitions, and there are also different meanings in different languages. However, many respondents intuitively differentiated between the two terms – by ascribing to them different levels – or "types" (e.g. ownership vs. spatial relationship) – of privacy.

[5] For commercial trade-offs, interviewees were asked whether they would disclose their phone number, address, date of birth, marital status, income, number and age of kids, their spouse's email address, their home insurance, life insurance, and their ID card number.

(d) The information requested was considered as "not relevant" for the website owner – something "they don't need to know", and it was not understood by interviewees why website owners would want such information.

Although it is not possible to compare different levels of willingness to disclose information between countries, it appeared that the interviewees in most countries are more restrictive in online than in offline situations, to different degrees in different cases. A majority outlined their uncertainty about what is happening to their personal data online and who is holding it and possibly sharing it with unknown others[6]. Interviewees from Spain, France and Italy were particularly critical of those with whom their information was being shared. . Interviewees from Romania were more willing to disclose personal information online than was generally the case in other countries, as they appeared to feel a certain obligation to provide personal information in the registration process for online accounts – even if the information requested was not mandatory[7].

Finally, being engaged in UGC usage did not necessarily go alongside a greater willingness to disclose information for commercial trade-offs, and being open to commercial trade-offs was not visibly linked to a more "generous" disclosure of personal and private information on UGC sites.

[6] See also section 3.3.1 below for a further elaboration of this point.

[7] For further details about this specific behaviour see the country report for Romania.

3.3 Privacy Matters

3.3.1 Which Privacy matters: Awareness and (Non-)Acceptance

Generally, the results in this study confirm the results of an earlier quantitative study carried out by the CONSENT project (work package 7) on user awareness and, particularly, the acceptance of the use by website owners of personal information disclosed by users on UGC websites. There is a considerable disparity between the awareness of, and reaction to, some common website practices, such as the customising of content and advertising, and practices that are less well known such as the sharing or selling of UGC users' personal information.

Interviewees in most countries[8] were aware of the use of user information by website owners to customize content and advertising seen by users. The majority of interviewees accepted this practice as a commercial trade-off, i.e. as "the price to pay" for a free service, or considered it as "normal" – or at least "inevitable". A number of interviewees even perceived it as an ingenious marketing strategy and could see its potential usefulness as some offers may be of interest to users. Some respondents also outlined that they felt this practice to be safe because it was "all automatic", i.e. the information gathering process was run by a computer – not a "real" person. However, the customisation of content or advertisement was *not* accepted if the data used were based on private communication between friends – such practice was explicitly perceived as an invasion of privacy. Additionally, for some interviewee their acceptance of this practice was subject to the customisation not dominating the website, not being "aggressive" nor being used for subliminal content – in which case a substantive loss of control was felt.

Generally, it appeared that most interviewees fluctuate in their attitudes and perceptions between disliking this practice, a perceived need to monitor it, accepting it as a commercial trade-off, and appreciating potentially positive effects. But some slight feelings of discomfort remain, with interviewees perceiving it also as something "weird" and confusing due to their lack of understanding of the underlying technical process; and a feeling that it may represent a form of "censorship" of information which could result in distrusting one's own judgments as they would be based on incomplete information.

The general acceptance of the customization of content and advertising described above applied to the majority of interviewees in most countries. In Denmark and the UK this does not apply. Here, the majority of interviewees did not accept the practice of the customization of content and advertising. They strongly felt that it represented an interference in their private life, infringing on their privacy, and linked it to the idea of surveillance. In the case of the UK this may be linked to many of the interviewees not being aware of this practice and, thus, rejecting it when first leaning about during the course of the interview.

[8] With the exception of Romania, Bulgaria and Slovakia where only a minority of interviewees was aware of this practice; in the Czech Republic and the UK half of the interviewees were aware of this practice. In the CONSENT online survey carried out as part of work package 7, 72% of all respondents were aware of the customising of content, and 79% were aware of the customising of advertising.

Most interviewees were not aware or only vaguely aware of the website owners' practice of sharing and selling personal user information to third parties[9]. This practice was mostly deemed unacceptable due to a fear of losing control; not only at the point of first information disclosure and when using the website, but also fearing the possibly uncontrollable use by third parties at any later point in time. The interviewees clearly stated that they wanted to decide themselves which data would be shared or sold, when and to whom – even if their information was anonymised. They particularly expressed feelings of uncertainty that their information may be used in a different way than what they had initially given permission for, expressing their unease that users' perceptions of privacy may differ from those of website owners.

The strongest emotional reactions to the practice of websites sharing and selling personal user information to third parties could, again, be observed with interviewees in the UK. They felt "angered" and "betrayed"; not only by private companies who carried out this practice but, partially, also by public institutions and the government as they saw such a practice as ultimately affecting their rights as citizens. In Romania there was a similarly strong rejection of the practice of websites sharing and selling personal user information to third parties. However, in this case this was linked to perceptions of helplessness and lack of power in controlling either public surveillance or the commercial practices of large private market players. This perceived lack of control, experienced in both offline and online situations, appeared to result in resignation, or even passive adaptation, rather than discomfort which would trigger reactions.

In contrast to the findings in all other countries, interviewees in the Czech Republic, who were predominantly low-frequency UGC users, showed a considerably higher level of acceptance of the practice of websites sharing and selling of personal user information to third parties with the condition of being asked for consent. These interviewees also exhibited a strategy of intended ignorance – they were aware that they lacked knowledge in this area but had no intention of rectifying this.

The vast majority of interviewees in all countries other than the Czech Republic expressed their deep discomfort with the practice of sharing and selling user information. Even though some of them described their fascination with the underlying technical possibilities, such feelings of possible admiration of the technology were overruled either by the extensive uncertainty about imagined as well as not yet imaginable consequences associated with this practice or by the perceived violation of a social norm.

[9] This is consistent with the results from the CONSENT online survey in which 61% of respondents were aware of website owners' sharing user information and 54% were aware of the selling of information, but only 7% of respondents accepted these practices.

3.3.2 How Privacy matters: Protective Measures

Disclosure strategies and measures taken to protect privacy online varied from country to country. The use of nickname was common with a majority of interviewees – except in Romania and Slovakia where it appeared to play a minor role. However, using nicknames was in many cases linked to a preference for anonymity rather than to the protection of privacy. It was meant to "disconnect" the link between the information revealed online and the user, rather than keeping the revealed information safe. At the same time, nicknames were often perceived as not being "fool proof". A number of interviewees expressed their awareness that one's real name was only one of many possible identifiers and not providing one's name was not sufficient protection against privacy violations.

The adaptation of privacy settings was mostly perceived as a more efficient measure to control access to personal information, though there were different levels of handling these settings. In most countries, the majority of interviewees chose a stricter privacy setting, but it seems that the possibilities and limitations of these settings are not widely known. However, in some countries (particularly Spain, France, Italy and Malta) the interviewees showed a strong awareness of the need to frequently re-visit and adapt their privacy settings, viewing this practice as their personal responsibility. At the same time, some of them also expressed the belief that there were no "guarantees" regarding potential future misuse of their personal information. This may indicate that there exists amongst some the realization that these protection measures may also serve the purpose of maintaining the "illusion" of being in control.

In contrast, a number of interviewees – particularly in Slovakia – left their privacy settings in default mode. This was either because they did not see the necessity to take substantial protection measures, or because they felt that measures such as privacy settings were "too technical". This suggests a low level of awareness and experience of possible data misuse.

Some German interviewees revealed another aspect of the use of privacy settings which suggests that basic differences in the way online social networks were used are associated with different perceptions of online privacy. Those interviewees who used SNS to organise and coordinate *all* their social contacts appeared to personalise their privacy settings, mostly, to a stricter level. But those interviewees who used SNS predominantly to allow first contacts and initial communication left their profile intentionally more open, explaining that privacy could not simply be turned "off" or "on" but was a matter of shades and degrees.

In summary, the most common practice described in all countries was to be "generally careful", "thinking carefully" and disclosing only "little" personal or private information. In some countries, particularly those where interviewees showed a high level of adapting privacy settings and using nicknames, interviewees additionally described strategies such as using incomplete or altered personal data, setting up separate accounts with different email addresses for different purposes, and creating different identities to achieve different levels of online privacy.

3.3.3 Making Privacy matter: Evaluating Privacy Policies

Despite the rather elevated level of adapting privacy settings which suggests a heightened awareness of the importance of online privacy, the majority of interviewees in most countries stated that they usually do not read privacy policies. The reasons given for not reading privacy policies can be divided into two categories: technical and content. On a technical level, the non-reading interviewees indicated that privacy policies were illegible due to being too long, written in text that is too small, and too difficult to understand. On the level of actual policy content, some non-readers additionally claimed that they were "always the same", or that they would already know the most important parts due to discussions in the media.

The three most prominent reasons for not reading privacy policies in those countries with a particularly high portion of non-readers are listed below.

A. The belief that carefully choosing individual privacy settings would be more efficient than, and a substitute for, the reading of privacy policies (UK).
B. A strong –user inertia that prevents the reading of privacy policies but co-existing with the belief that policies should be read. In this case respondents stated a perceived need to make it harder for themselves to accept privacy policies, being "forced" through a more comprehensive consent procedure which would move them closer towards an informed choice (Denmark).
C. A deep mistrust towards private and public institutions, linked to the belief that privacy policies would serve the primary purpose of protecting the website owners rather than the website users (Romania).

A number of interviewees, readers and non-readers, in almost all countries shared the perception in C above that privacy policies primarily serve the purpose of protecting the website owners rather than the website users.

Those interviewees who claimed that they mostly do read privacy policies strongly linked their policy reading to the reading and changing of privacy settings. These interviewees viewed the reading of privacy policies as part of a learning process that is indispensable if one wishes to assume responsibility for one's personal information and be able to take adequate protective measures. These interviewees would like to see changes in privacy policies such that there is a clearer separation between privacy-related and general issues, and the inclusion of educational aspects related to privacy.

However, the majority of interviewees who read privacy policies admitted that they would still sign up and open an account, even if they did not find the content they expected in the privacy policy, as they felt that there was no viable alternative to accepting the website's conditions. Those readers who perceived themselves as actively taking up responsibility for their privacy online stated that they would either contact the website owner and try to clarify any doubts they had about the privacy policy, would search for an alternative website offering a similar service but without formal registration (or less information requirements), or would sign up with fake personal data. Those who do this are likely to be a very small minority.

4. Conclusion

In the results obtained from interviews conducted with both UGC users and non-users in all partner countries, two distinct perceptions relating to personal data online are evident. Either generally elevated levels of perceived control or perceived lack of control over one's personal information.

Elevated levels of perceived control were mostly linked to:

A. the belief that the existing legal data protection framework provides sufficient protection (e.g. in Germany);
B. a limited experience of online privacy violation (e.g. in Poland); or
C. the extension of the prevailing offline conditions of perceived social order and protection by law to a "guaranteed" privacy online (e.g. Denmark).

Perceived lack of control was mostly based on either the concept of privacy being underdeveloped (e.g. in Romania or Bulgaria), and/or a perceived helplessness which was, often, masked as disinterest (e.g. in Romania, but also occurring in most other countries). Such helplessness, based on lacking both expertise and power, appeared to reinforce itself and tie users in a cycle of increasing passiveness, which may be more difficult to overcome than general user inertia.

It may be possible to devise public policy strategies to overcome user inertia by examining the attitudes, perceptions and reasons for action of those interviewees who described situations where inertia had been overcome and personal responsibility was taken. These are users who did read privacy policies, adapted their privacy settings or developed individual strategies to protect their privacy online.

As one very basic attitude, users who have overcome inertia and accepted personal responsibility for their online privacy appeared to accept that in the online environment there is no ultimate guarantee for privacy protection, and that there remains an inherent uncertainty which cannot be resolved. Only once this uncertainty is accepted, does it appear possible to go a step further and assume the rights and obligations of "digital citizenship". In order to overcome inertia and accept personal responsibility for online privacy there appears to be the need to acknowledge that the online environment has certain risks, but also offers a number of opportunities; and, like in the offline world, citizenship provides empowerment but requires responsible behaviour towards others as well as towards oneself.

Apart from the more formal legal rights and obligations mentioned in the previous paragraph, there are also social values, such as trust, or respect, that are well known and commonly accepted in the offline environment. Transferring these to the online environment was seen as an important, and desirable, step towards increasing privacy protection online. Those interviewees who had done so, whilst accepting the aforementioned uncertainty and the ongoing struggle for a power balance, expected to be given the choice to decide which UGC websites to use and which personal information to disclose to whom, when, and for how long – defining their own personal level of online privacy.

Acknowledgements

This research was carried out as part of CONSENT (Consumer sentiment regarding privacy on user generated content (UGC) services in the digital economy) a project that was funded by the European Union under the Seventh Framework Programme (2007-2013), Grant Agreement Number 244643.

Appendices

A. Interview Guidelines (English)

Instructions for Interviewers

As the intention of these interviews is to gain a deeper understanding of personal opinions, thoughts, feelings, experiences and behaviour towards privacy based on the quantitative results from WP7, it is crucial to allow the respondents to speak as freely as possible and allow them to develop their own chain of thought, rather than following a pre-defined yes/no or "multiple choice" pattern. Obviously, one of the main challenges for any interviewer conducting standardised open-ended interviews is to find the balance between allowing such openness *and* maintaining control – taking oneself back without losing the "red line" – and the wording of the interview questions is accounting for this.

However, conducting interviews about a complex subject will always remain a complex task, and the following practical recommendations are meant to help reducing at least some of the complexities involved.

Plan ahead: Make a definite appointment with the respondent in a location of her/his choice where she/he feels at ease, but keep in mind that it should be sufficiently private to allow for an interview without undue distractions or interruptions. Avoid tight time schedules, as feelings of pressure may – unwillingly – be passed on to the respondent.

Be familiar with the interview guidelines: Practice the questions beforehand, and read the questions-specific instructions (marked in italic letters) carefully. Stick to the guidelines and don't jump between questions.

Be familiar with the technical equipment: Make a short test recording before each interview to assure that the recording equipment is working fine and batteries are sufficiently charged.

Ask open questions: Particularly when probing an interviewee's response, it is tempting to ask suggestive questions (e.g. "So you think / don't think that…?"). Although not always possible, such yes/no questions should be mostly avoided. Attempt to remain asking open direct questions, and also use other probing techniques like empathy, expectant pauses or mirroring, giving the respondent sufficient time to elaborate.

Stay alert: Whilst it is important to be interactive, the interviewer's main task is to listen and observe throughout the conversation. It is also recommendable to remain alert and potentially make notes after the interview, as respondents often give crucial information immediately after the recording device is turned off.

Introduction	Briefing
ALL RESPONDENTS **Introduction** [about 5 min] - Thank you - Your name - Purpose - Confidentiality - Duration - How interview will be conducted - Signature of consent on consent form	**I would like to thank you for taking the time to meet me today. My name is----------and I would like to talk to you about the internet, what you like about it, what you dislike, and how you use it.** **As was mentioned when we set up this appointment, this interview is being carried out as part of the CONSENT project which is co-funded by the European Union. The CONSENT aims to gather views of internet users from all countries of the EU. If you wish I will give you more information about the CONSENT project at the end of the interview.** **Your opinion is very valuable for our study and will be taken into consideration when drawing up the final report.** **The interview should take less than one hour. I will be taping the session because I don't want to miss any of your comments. Although I will be taking some notes during the session, I can't possibly write fast enough to get it all down. Because we're on tape, please be sure to speak up so that we don't miss your comments.** **All responses will be kept confidential. This means your interview responses will only be shared with research team members and will ensure that any information we include in our report does not identify you as the respondent. Your name will not be connected with the answers in any way.** **Please read and sign this consent form. Do you have any questions on that?** **Remember, you don't have to talk about anything you don't want and you may end the interview at any time. Is that OK?** *Running Total: 5 min*
Objectives	**Questions**
ALL RESPONDENTS **Word-association exercise** [about 3 min] - establish top of	**Q.1 To start off we are going to play a short game/carry out a short exercise: I will read out a word and I would like you to say the first couple of things that come to mind/pops into your head when you hear the word. Let's try an example first: What is the first thing that comes to mind if I say the word "summer"? Anything else?** *Encourage respondents to use short phrases or single words and to*

mind associations with privacy	*avoid lengthy descriptions and statements.* *Test words:* **honesty, internet, work, family, privacy** *Running Total: 8 min*
ALL RESPONDENTS **Willingness to disclose personal information in various situations.** [about 8 min]	**Q.1.1Now let's talk about something a little different. I would like you to imagine you are on a plane and the person next to you, somebody you don't know and who you are unlikely to ever meet again, is a really talkative member of the same sex about your age. He/she starts talking about different things and after 15 minutes he/she asks you whether you were single, married or in a relationship, what would you tell her/him?** *Let respondent reply freely, and if they don't give reasons why, only then ask further why/why not.* **Q.1.2 What if he/she asked you about how much you earn What would you do?** *Let respondent reply freely, and if they don't give reasons why, only then ask further why/why not.* **Q.1.3 And what if they would tell you they can use their ID card number to choose lottery numbers to play. He/she asks you what your ID card number is. What would you do?** *Let respondent reply freely, and if they don't give reasons why, only then ask further why/why not.* **Q.1.4 Now let's imagine that instead of this talkative fellow passenger, you were asked the same questions by a friend who you meet a few times a year. What would you do?** *Probe about each of: whether you are single, married or in a relationship, how much you earn, ID card number. And in each case whether respondent would say the truth and why/why not* *Running Total: 16 min*
ALL RESPONDENTS **Internet experience and attitudes** [about 5 min]	**Q.2 Let's talk a bit more about the internet now, how long have you been using the internet?** **Q.3 What do you love most about the internet?** **Q.4 What do you dislike most about the internet?** *Running Total: 21 min*
ALL RESPONDENTS **Underlying beliefs & attitudes to commercial/privac**	**Q.5 Imagine that you are visiting a website of a discount club, for example a site similar to Groupon <***or similar, please choose the one most appropriate for your country***>. The club offers up to 50% discounts on different consumer products and services (e.g. books, travel, household goods, and fashion items) to its**

y trade-off [about 5 min]	**members. The site is currently running a promotion and giving a discount up to 75% to all visitors who provide the site with more information than the standard name and email. Which information would you be willing to provide this website to get this up to75% discount offer?** *Start reading out list:* **phone number, home address, date of birth, annual income, marital status, number of kids, age of kids, ID or passport number, email address of partner or spouse, life insurance status, home insurance status** *For items that respondent is <u>not</u> willing to provide information about to the website probe reason:* **Q5.i Why not?** *Or* **Why wouldn't you give your...** *Running Total: 26 min*
ALL RESPONDENTS **Internet usage** [about 2 min]	**Q.6 Please tell me a little about the internet websites you use in a typical week and what you use them for.** *Probe if Internet activities describe above (including usage of UGC and SNS) have an impact on the respondents' lifestyles, habits and social relationships (just 2 minutes for this question, so do not go into too many details).* *Running Total: 28 min*
ALL RESPONDENTS **UGC usage** [about 5 min] - Establish whether UGC user or non-user - Establish whether SNS user - Establish UGC site used most frequently - Provides link to findings from online questionnaire *Show card A*	**Q.7 This is a list of some websites** <*show list of UGC sites used in each country for WP7* >**. Could you please tell me whether you have accounts with (not just visit) any of them and if you do have an account how often you log in?** <*Make a note which whether respondent uses Social Networking Site and if not which UGC website respondent uses most*> *Show card A:* **A. Social networking website such as Facebook, <Local SNS used in WP7>** **B. Business networking websites such as LinkedIn, Xing.com** **C. Dating websites such as parship.com** **D. Websites where you can share photos, videos, etc., such as YouTube, Flickr** **E. Websites which provide recommendations and reviews (of films, music, books hotels etc), such as last.fm, tripadvisor** **F. Micro blogging sites such as twitter** **G. Wiki sites such as Wikipedia, myheritage** **H. Multiplayer online games such as secondlife.com, World of Warcraft**

	Probe how much time is spent on social networks and UGC services daily/weekly (if not established already in Q6) *Running Total: 33 min*
RESPONDENTS WHO DO <u>NOT</u> USE OR NO LONGER USE UGC SITES IN Q7 **Reasons for not using UGC sites** [about 3 min]	**Q.8 Why don't you have accounts with any of these sites, or why did you cancel or don't use them anymore? Anything else?** *Probe fully, but make note of first and second reason given.* *We are interested in exploring further any reasons that relate to respondents' concerns about:* *- the consequences of giving information online,* *- how information about them is used,* *- whether UGC sites can be trusted, and* *- any other issue relating to privacy.* *<u>If privacy/information use/trust related issues not mentioned as a reason for not using (anymore)UGC sites ask:</u>* **Q.9 For what reasons may you be likely to open an account – or not open account - with any of these sites soon?** *Allow respondents to speak freely, but then gently probe to establish if respondent feels any pressure to open a UGC account;* *<u>If any privacy/information use/trust related issues mentioned ask:</u>* **Q10. You mentioned that one of the reasons (the reason) you don't use UGC sites is <***whatever respondent said that relates to privacy/information use***>. Can you tell me a bit more about what in particular concerns you**? *Probe <u>in depth</u> to determine* *i. what aspect of UGC sites respondent finds unacceptable, and why;* *ii. beliefs about how internet sites use information;* *iii beliefs about what UGC sites are for.* *Running Total: 36 min*
RESPONDENTS WHO USE UGC SITES IN Q7 **UGC sites - Motivations & Usage** [about 6 min] Establish: - motivations for	**Q.11 Why did you start using** *<Social Networking Site, if used. If respondent does not use Social Networking site, then UGC site in Q7 used most frequently>***?** *Probe to determine key motivations for using site.* **Q. 12 During all of the time that you've been using these sites, what information about yourself have you put on the site/sites?** *Allow respondents to take their time and reply in their own words but probe for: name, home address, photos of you, photos of family and friends, audio-video recordings, medical information, hobbies, sports, places where you've been, tastes and opinions, etc*

UGC use - willingness to share information - beliefs & attitudes on different types of information - motivations for settings of who can view information	**Q.13 Who can see your profile and/or your photos?** *Probe* **Why have you set things up in that way?** **Q.14 Have you ever regretted posting some information on one of these sites?** *If yes:* **Q.15 Can you tell me a little bit about it...what happened? Why did you regret the posting?** *If respondent <u>does not</u> mention commercial info & negative effects, then also ask 16.1 and 16.2* *If no:* **Q.16 Could you imagine a situation when you might regret it?** *Probe to determine whether lack of concern about respondent's own posting is due to:* *i. respondent posting little information, or* *ii. always thinking carefully before posting, or* *iii. thinking that it is no problem that everybody has access to information about them* *If NOT i and ii then ask:* **16.1 Do you receive commercial info that you think is a result of the personal information that you have posted? If yes, how do you feel about this?** *Probe to determine exactly:* *i. if the respondents are aware of consequences of putting information online* *ii. why some are more acceptable than the others* *iii. do people accept that receiving commercial info is part of the commercial trade-off for using the service* **16.2 What do you think can happen (for example regarding job selection, reputation) as a result of personal information you have posted?** *If Yes-* **How do you think this will happen?** *If No-* **Why don't you think this is possible?** *Probe to determine exactly how the respondents think about other people using their own information posted on UGCs. Use a neutral tone to allow both positive and negative reactions.* *Running Total: 42 min*
ALL RESPONDENTS **Usage of**	*If not previously established up to this point* **Q.17 Have you yourself ever used an alias or a nickname when giving information online? In what case/s and why? Or, if you**

aliases/nicknames [about 2 min] - explore attitudes towards revealing personal information in different situations	**haven't, what do you think about it?** *Probe more in detail.* *Running Total: 44 min*
ALL RESPONDENTS **Attitudes towards use of personal information by websites** [about 8 min] *Show card B*	**Q.18 The information users include in their account or profile on a website can be used by the website owners for a number of purposes, such as to customize the content and advertising that users see, to send them emails, to gather in-depth personal information about them etc. Did you know this when you signed up with a website (or UGC/SNS)? What do you think of it?** *Make a note whether respondent was aware of purposes and probe to determine attitude to use of users' information for each of the following:* *Show card B:* 1. *customize the advertising you see (show you only advertising for things/services that likely to interest you)* 2. *share information (which could be linked to your name) about your behaviour with other parts of the company* 3. *sell information (not linked to your name) about your behaviour to other companies* *For <u>each purpose</u> probe respondent for the reason behind finding the use acceptable/unacceptable.* *If not already mentioned, for any purpose respondent finds unacceptable ask:* **Q.19 Under which conditions, if any, would you find it acceptable for users to give information about themselves to be used by a website for** *< purpose respondent finds unacceptable>***?** *Probe to determine whether respondent would accept a ticket in a sweepstake/lottery, points on website such as Facebook points, a share of profits from the website, money.* *Running Total: 52 min*
ALL RESPONDENTS **Attitudes towards & behaviour on privacy policies.**	**Q20 What do you think about privacy policies of the UGCs/SNS that you are using? Did you read them before you signed up?** *(choose one as an example, If no to Q 7,then any other website that you use frequently)* *If yes* – **what would you look for? If you didn't find what you have looking for, what would you do?**

[about 4 min]	*Probe to determine:* *- if people really read the privacy policy;* *- what (presence/absence of some feature? reassurance?) they are looking for when they do read privacy policies; and* *- what they do if what they are looking for isn't in the policy (carry on using the website anyway? not start/stop using it?)* *Running Total: 56 min*
ALL RESPONDENTS **Thank & close**	**That's all from me, is there anything else you would like to add?** *Hand out incentives if used* *Inform about the next steps, give more information about CONSENT project if respondent wishes* **Thank you very much for your valuable contribution to our project!** *Total: 60 min*

B. Pre-Analysis Template

Interview Country: _____ **Interviewer (name):** _____
Date: _____ **Interview number:** _____

Interviewee age: _____ **Gender:** □ **Female** **Location:** □ **urban / suburban**
□ **Male** □ **rural**

SNS/UGC usage: □ **SNS/UGC user**
□ **UGC (non-SNS) user**
□ **SNS/UGC non-user**

Description of interview situation / overall impression:

Here, the idea of such general description is to provide a sense of how the interview went, and a general feeling of how the interviewee behaved during the interview. The interviewer (and/or the person transcribing the interview / filling out the template) is encouraged to reflect upon the general tone (e.g. relaxed, stiff), emotional expression (e.g. enthusiastic, reserved, interested, keen) and language use (e.g. formal/informal, precise, casual choice of words) of/by the interviewee as well as any specific content that is considered particularly important, e.g. highlighting contradictory statements, shifting perspectives and perceived ambivalences. Any quotes are particularly welcome!

A. Word Associations (Q1)

	Word Associations *(Please use single words or short phrases)*
Honesty	
Internet	
Work	
Family	
Privacy	

B. General Attitudes and Behaviour towards Disclosure of Personal Information

Willingness to give the following information:

To "Strangers"	**Yes**	**No**	**Other** *(please specify)*	**Reasons**
Marital Status (Q1.1)				
Income (Q1.2)				
ID Number (Q1.3)				

To Friends	**Yes**	**No**	**Other** *(please specify)*	**Reasons**
Marital Status (Q1.4)				
Income (Q1.4)				
ID Number (Q1.4)				

Additional Quotes:

C. Years of Internet Usage ☐ **(Q2):**

D. General Internet-related Attitudes

Positive Aspects of the Internet ("love most") (Q3)	e.g. broadness of information, entertainment, worldwide networking, source of inspiration
Negative Aspects of the Internet ("dislike most") (Q4)	e.g. misleading information, meaningless chatting, source of distraction, peer pressure to use SNS websites

Additional Quotes:

E. Commercial "Trade-Off's" (Q5, Q5.i)

Information the interviewee would be willing to provide for a large discount on online purchases or services:

	Yes	No	Reasons
Phone Number			
Home Address			
Date of Birth			
Annual Income			
Marital Status			
Number of Kids			
Age of Kids			
ID / Passport Number			
Email address of partner/spouse			
Life Insurance Status			
Home Insurance Status			
Other			

Additional Quotes:

F. Everyday Internet Routines (Q6, Q7)

Frequency per day/week of

	Frequency	Potential Impact on lifestyle, habits, social relationships
Checking Emails		
Using Search Engines		
Using SNS websites *(which?)*		
Using other UGC websites *(which?)*		
Checking News		
Other *(please specify)*		

Additional Quotes:

G. SNS/UGC-related Perceptions, Attitudes and Behaviour

G.1 Interviewee holding / not holding accounts with one or more of the following sites (Q7, Q8, and Q11):

	Yes	No	Reasons for closing / not using the account anymore	Reasons for starting to use the account (Q11)
SNS websites *(e.g. Facebook, local SNS websites)*				
Business networking websites *(e.g. LinkedIn)*				
Dating websites *(e.g. parship.com)*				
Photo/video sharing websites *(e.g. Flickr,*				

YouTube)				
Websites providing reviews *(e.g. tripadvisor)*				
Micro blogging sites *(e.g. Twitter)*				
Wiki sites *(e.g. Wikipedia)*				
Multiplayer online games *e.g. World of Warcraft)*				

Additional Quotes:

G.2 Likeliness of SNS/UGC <u>non</u>-users to open an Account in the future (Q9)

	Likely	**Not so likely**	**Reasons**
SNS websites *(e.g. Facebook, local SNS websites)*			
Business networking websites *(e.g. LinkedIn)*			
Dating websites *(e.g. parship.com)*			
Photo/video sharing websites *(e.g. Flickr, YouTube)*			
Websites providing reviews *(e.g. tripadvisor)*			
Micro blogging sites *(e.g. Twitter)*			
Wiki sites *(e.g. Wikipedia)*			

Multiplayer online games *e.g. World of Warcraft)*			

Additional Quotes:

G.3 Specific Privacy Concerns of SNS/UGC non-users (Q10)

Please quote the interviewees response to question 10; if she/he doesn't have any concerns regarding privacy in the context of opening/not opening or closing any SNS/UGC account, please indicate the reasons why (if given by the interviewee).

G.4 Personal Information Disclosure on UGC websites (Q12, Q13)

Name / Type of website		**Type of information disclosed**	**Reasons for disclosure**	**Disclosure Strategies** *(e.g. leaving questions blank, looking for similar websites that require less information)*
		Name		
		Home address		
		Photos of the interviewee		
		Photos of the interviewee's family & friends		
		Audio-video recordings		
		Medical information		
		Hobbies		
		Sports		
		Places where the interviewee has been		
		Tastes and opinions		
		Other		

Additional Quotes:

G.5 Privacy Settings (Q13)

Name / type of website	**Form of setting** *(e.g. stricter, less strict, limiting who can see personal information, (de-)activating newsletters / commercial offers, further usage of personal information provided)*	**Motivation for this form of privacy setting**
(add lines if required)		

Specific Quotes:

G.6 Consequences of Disclosing Personal Information (Q14, Q15, Q16, Q16.2)

	Situation where the disclosure of information was regretted	**Consequences**
Actual (own) experience		
Experiences of others		
Imagining future situations		

Specific Quotes:

G.6.1 Commercial Offers as a result of disclosing personal information (Q16.1)

Receiving commercial offers as a result of having disclosed personal information is		Reasons / Conditions
Acceptable		
Not acceptable		
Acceptable under conditions		

Specific Quotes:

G.7 Using an alias or a nickname (Q17)

		Reasons for/against using an alias or nickname
Yes		
No		

Specific Quotes:

G.8 Interviewee's Awareness of website owners using personal information for a number of purposes (Q18, Q19)

	Awareness		How did the interviewee learn about this	Attitude	Reaction / Resulting Behaviour
Customising the content and advertising users see	**Yes**	☐ Before opening the account ☐ After opening the account		☐ Acceptable ☐ Not acceptable ☐ Acceptable under conditions	
	No				
Passing on personal information to third parties without permission	**Yes**	☐ Before opening the account ☐ After opening the account		☐ Acceptable ☐ Not acceptable ☐ Acceptable under conditions	
	No				
Sending unwanted emails / newsletter	**Yes**	☐ Before opening the account ☐ After opening the account		☐ Acceptable ☐ Not acceptable ☐ Acceptable under conditions	
	No				
Selling personal information to other companies	**Yes**	☐ Before opening the account ☐ After opening the account		☐ Acceptable ☐ Not acceptable ☐ Acceptable under conditions	
	No				
Gather in-depth information about users	**Yes**	☐ Before opening the account ☐ After opening the account		☐ Acceptable ☐ Not acceptable ☐ Acceptable under conditions	
	No				

Specific Quotes:

G.9 Privacy Policies (Q20)

G.9.1 Reading privacy policies

Reading privacy policies before signing up		Reasons
	Mostly yes	
	Mostly not	

G.9.2 Content of privacy policies

Beliefs about privacy policies ("What do you think about privacy policies")	
Content expected to find ("What do you look for")	
Action taken if not found	
Other comments	

Specific Quotes: