Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies

Bart Custers[*], Simone van der Hof, Bart Schermer

Leiden University, eLaw – Centre for Law in the Information Society
Steenschuur 25, 2311 ES Leiden, The Netherlands
[*]E-mail address: bartcusters@planet.nl

ABSTRACT

Social media process (sometimes large amounts of) personal data of their users, usually on the basis of informed consent. In this paper, a comparison is made between, on the one hand, existing practices of social media regarding informed consent for using personal data of users and, on the other hand, user expectations with regard to privacy and informed consent. The comparison is made on the basis of a set of criteria for informed consent distilled from an analytical bibliography. Next, the privacy policies of a selection of eight social network sites and user generated content sites were analysed using this set of criteria for informed consent. User expectations regarding these criteria were derived from survey results of a large EU-wide online survey (N=8621, 26 countries) on the awareness, values and attitudes of social media users regarding privacy. Not all criteria are important to users, but most criteria that are important to users can be found in most privacy policies.

Keywords: informed consent, privacy policy, user expectations, social media

1. INTRODUCTION

In recent years, social media have attracted a large increase of users. Lots of people are moving online to use both User Generated Content websites (UGCs), like YouTube and Wikipedia, and Social Network Sites (SNSs), like Facebook and Google+. However, since the success of many of these websites depends to a large extent on the disclosure of personal data by its users, some concerns about privacy issues have been raised. Although it may be argued that users voluntarily sign away their privacy by using these social media when creating accounts and putting their personal data online, it is not clear how consent actually works in these situations.

The research results described in this paper are part of a larger research project called CONSENT (See: www.consent.law.muni.cz). [1] This project examines how consumer behaviour, and commercial practices are changing the role of consent in the processing of personal data. Part of the project is to investigate the current practices of social media, user expectations with regard to privacy and consent and the legal provisions for informed consent. In previous research, the extent to which legal provisions exist both in the existing and the proposed legal framework of EU personal data protect was investigated (Custers et al. 2013). A gap analysis was made between user expectations regarding a set of criteria for informed consent (presented below) and the availability or absence of related legal provisions in both the current and the proposed legislation.

[1] The project was co-funded by the European Union under the Seventh Framework Programme, grant number Grant agreement No.: 244643.

In this paper, current practices of social network sites and user expectations with regard to privacy and informed consent are compared. Practices of eight social media sites were examined by analysing their privacy policies. User expectations were predominantly derived from survey results of a large EU-wide online survey on the awareness, values and attitudes of social media users regarding privacy set up and executed by one of the partners in our research project. The comparison between the current practices and the user expectations is based on a set of criteria for consent distilled from an analytical bibliography.

This paper is structured as follows: in Section 2 the set of criteria for consent that was used for our analysis is set forth, in Section 3 and Section 4 the results of the analysis of the privacy policies and the user expectations are presented respectively, in Section 5 these results are compared and discussed, and, finally, in Section 6, conclusions are provided.[2]

2. CRITERIA FOR CONSENT

Consent is an important notion in our society. The notion of consent is largely based on the principle of (respect for) autonomy which is, in its simplest form, to respect people as individual centres of control over their own lives. It is generally held that (at least) two conditions are essential for autonomy: a capacity for intentional action and independence of controlling influences. A lack of consent may imply a violation of the principle of autonomy (e.g., Shultz, 1996, Gold, 1996), However, relying on consent only to safeguard autonomy may not be enough (McCrystal and Barnes, 2002). Consent is also an important notion in social media use, since it is based on the idea that individual social media users make conscious, rational and autonomous choices about the disclosure of their personal data. But whether data subjects are always capable of making these choices and willing to do so in practice is questionable. There is mounting evidence that data subjects do not fully contemplate the consequences and risks of personal data processing. Although people seem to manage their information and self-presentation on the basis of context and audience (Goffman, 1959), social network sites tend to aggregate contexts, often making the actual audience difficult to determine (Litt, 2012, Hargittai and Litt, 2013). When online, it seems that many data subjects simply consent whenever confronted with a consent request (Böhme and Köpsell, 2010). Therefore, there is growing scepticism regarding the effectiveness of notice and consent in the context of data processing. (Pollach, 2007, Acquisti, 2009, Adjerid et al., 2013, Solove, 2013). According to Nissenbaum (2011) there is considerable agreement that this model has failed. She argues that there is a transparency paradox: efforts are being made to meet the need for brief and clear privacy policies, since too detailed information on data flows, conditions, qualifications and exceptions are unlikely to be understood, let alone read. However, an abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry significance (Toubiana and Nissenbaum, 2011).

In order to determine more precisely how informed consent should look like in social media use, a set of criteria for consent was developed a the basis for the compare and contrast analysis of our research. These criteria were based on an analysis of a bibliography on existing privacy criteria (Mommers & Kielman, 2010), an analysis of the concepts on which legal obligations with regard to consent are based (Nazarek, 2012) and further social and psychological elements pertaining to individual users, including user needs, interests and preferences, derived from the idea that consent is an instrument to equip people with control over their own lives (autonomy) and over their personal information (privacy or informational self-determination) (Westin, 1967).

[2] Some of the research results presented here, were preliminary presented at a conference (Custers et al., 2013).

In general, the process of providing consent is only considered fair when the person involved is properly informed of what exactly he or she is consenting to and, to some extent, is (made) aware of the consequences such consent may have. This is indicated with the term *informed* consent. Informed consent is used to ensure that people make well-considered decisions. Hence, generally the condition is added that consent has to be informed consent. In this paper, by consent we mean informed consent. Although providing information is generally accepted as a legal or ethical requirement for consent, it may not always be clear how much information should be provided, data subjects may not take notice of (i.e., may not read or listen to) the information provided, or, if they do, may not understand (all of the) information provided. These are serious concerns and there is research indicating that the levels of awareness and concern about privacy issues is low. Turow (2005) found wide levels of misunderstanding. For instance, consumers understood the mere presence of privacy policies as data protection. Focused more specifically on SNSs, Acquisti and Gross (2006) found that most users in their Facebook study were unaware of data collection rules. However, there is also recent research that indicates that users are aware and concerned about their privacy. boyd and Hargittai (2010) reported on a substantial number of young Facebook users who were aware and concerned about potential privacy threats, contrary to the conception that young people do not care about privacy.

The basic model for informed consent consists of two steps: asking consent by a data controller and providing (or denying) consent by a data subject. When taking a closer look at both steps, it can be seen that each of these steps contains a lot more actions. The first step, i.e., asking for consent, involves that the data controller provides also information that a data subject needs in order to be able to make a decision. This is illustrated in Figure 1. This information may concern both the content of consent (what is exactly consented to) and the process (how to consent).

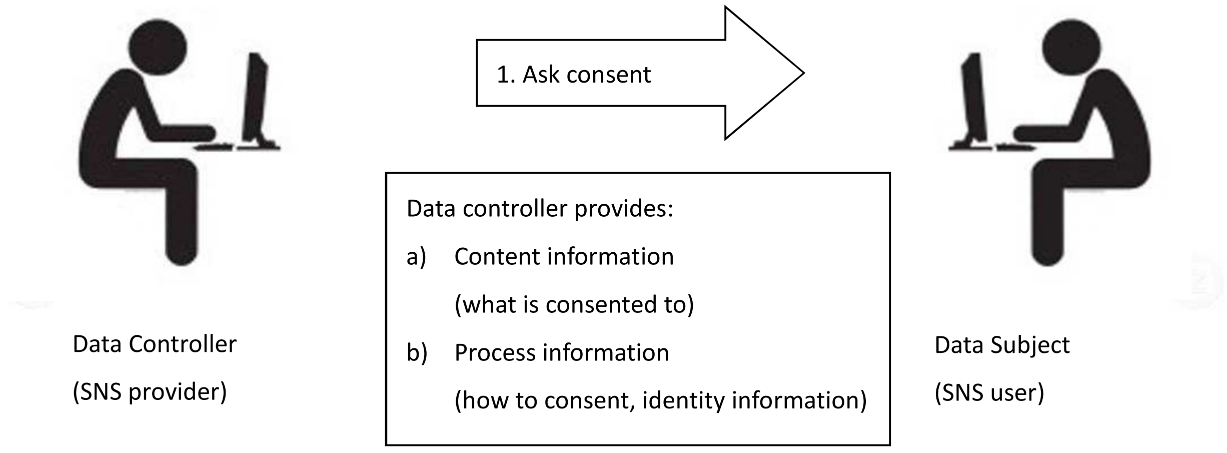

Figure 1: The first step, asking for consent, involves providing further information on the content of consent and the process of how to consent.

The information on what is consented to may include a further specification of the request, for instance, including details on which personal data are collected and for which purposes. It may also include further information on the consequences of giving consent, such as a data subject's rights and obligations.

The information on how to consent may include further information on the process, such as identification of the data subject and data controller, the way in which consent is to be provided (e.g., orally or written, ticking a box, submitting a form, etc.) and information on how consent may be revoked at a later stage.

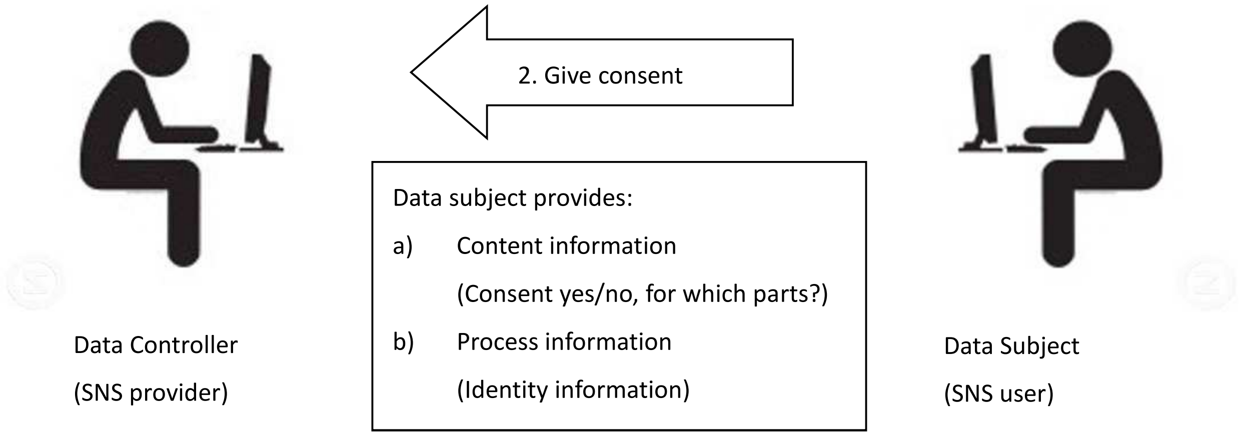

Figure 2: The second step, giving consent contains providing content information and process information.

The second step, i.e., giving (or refusing) consent, is illustrated in Figure 2. The information provided by the data subject concerns content information (is consent provided or not, for which parts is consent provided, is the consent provided subject to particular conditions, etc.) and process information (including the identity of the data subject and, in some cases, further information about the data subject, such as his age, authorization or bank account number or credit card details).

In Table 1 it is shown which criteria were used to determine whether there is informed consent. We distinguish between criteria that focus on the consent itself (i.e., who can give consent and how can consent be given?) and criteria that focus on the condition that the consent is in fact informed consent (i.e., what information should be provided and how should it be provided?).

Table 1: Set of criteria for consent

Criteria regarding the decision to consent	Criteria regarding the person who consents	C1.1	Is the person who consents an adult? If not, is there parental consent?
		C1.2	Is the person who consents capable to consent? If not, is there a legal representative who consents?
		C1.3	Is the person who consents competent to consent?
	Criteria on how to give consent	C2.1	Is the consent written?[3]
		C2.2	Is the consent partial or full? In case of partial consent, does the consent cover the purpose?
		C2.3	Is the consent reasonably strong?
		C2.4	Is the consent an independent decision?
		C2.5	Is the consent up to date?
Criteria regarding the well-consideredness of the decision to consent	Criteria regarding what information should be provided	C3.1	Is it clear which data are collected, used and shared?
		C3.2	Are the purposes clear?
		C3.3	Is it clear which security measures are taken?
		C3.4	Is it clear who is processing the data and who is accountable?
		C3.5	Is it clear which rights can be exercised? Is it clear how these rights can be exercised?
	Criteria regarding how information should be provided	C4.1	Is the information provided specific and sufficiently detailed?
		C4.2	Is the information provided understandable?
		C4.3	Is the information provided reliable and accurate?
		C4.4	Is the information provided accessible?

Although almost all of the criteria in Table 1 are backed by legal provisions (for an overview, see Custers et al. 2013) and by literature, we would like to stress that there are many differences in the interpretation and implementation of these criteria. For instance, the rather straightforward criterion whether a person who consents is a minors or an adult may yield different answers in different settings. E.g., in some countries, a 16-year old is allowed to drive a car, whereas, an 18-year old is allowed to get married without parental consent. Many minors are nowadays using social media and the proposed EU data protection legislation sets the age threshold for parental consent at thirteen years old (Hornung, 2012).

Despite these complications, determining whether someone is an adult is much less complicated than assessing some of the other criteria mentioned in Table 1 that have some inherent uncertainty. For instance, determining whether the information provided is specific and sufficiently detailed, may depend on the purposes for which the data is processed and the person to whom the information is provided. As such, some of the criteria are intertwined, as the necessary level of detail (C4.1) may depend, among other things, on the person who consents (C1.1-C1.3), the data that is collected and for which purposes (C3.2-C3.3) and understandability of the information provided (C4.2).

Nevertheless, we consider the criteria in Table 1 important and necessary elements for consent. In summary, if one of the criteria is not met, the consent is flawed. From a legal perspective, the only criterion that is not typically required is the requirement that consent is

[3] By written we mean information in both physical documents and electronic formats

written. In the context of social media, however, we have not encountered any forms of consent that were not written. Since our research focuses on privacy policies, we decided to include the criterion of written consent in our analysis.

Apart from the criteria in Table 1, it should be mentioned that there may be other factors which may mitigate the ability of social media users to make informed consent decisions despite the provision of all legally relevant information. An example may be that users may be confronted with so many consent decisions that they may have no time to really consider each decision carefully (Schermer et al., 2014).

It is important to note that in the following sections we did not assess to which extent privacy policies *meet* the criteria in Table 1. We merely assessed whether these criteria are *mentioned* or *addressed* in the privacy policies.

3. ANALYSIS OF PRIVACY POLICIES

Social media websites generally present the information that they consider necessary for their users to be enabled to make informed decisions in their privacy policy. This is a document or page on their website. Informing data subjects about the goals of data processing is a legal requirement under EU data protection law. While the legislation does not specify how this information must be presented (i.e., having a privacy policy is strictly speaking not a legal requirement), most data controllers present the information via a privacy policy. Some social media websites choose to present the information for informed decision-making in the user agreements, in their terms and conditions or somewhere else on their website. Within the EU there exists a considerable amount of legislation regarding the conditions of fair processing of personal data. For more details, see Bygrave (2002). It should also be mentioned that the EU legislation on personal data protection is currently under revision (Hornung, 2012).

For the scope of our research we considered both Social Network Sites (SNSs) and User Generated Content Sites (UGCs) as social media. The Article 29 Data Protection Working Party (WP29)[4] defines SNSs as online communication platforms which enable individuals to join or create networks of like-minded users. There is no widely accepted definition of UGCs, but the OECD defines user generated content as content made publicly available over the Internet, which reflects a certain amount of creative effort and which is created outside professional routines and practices.[5] Since many UGCs deal with content produced interactively by individual users that may affect their privacy, we included these in our research.

Using the criteria for consent in Table 1, we analysed the privacy policies of eight social media websites with regard to the asking for and providing (or denying) consent. Since, in some cases the criteria are not discussed in the privacy policies, we also considered the user agreements or other terms and conditions available on the websites. The eight websites analysed were LinkedIn, Wikipedia, Facebook, YouTube, Habbo, Hyves, Relatieplanet and Twitter. These websites were selected from an extensive list of Social Network Sites and User Generated Content sites available in the European Union (Krügel, 2010). The main criteria to categorize this list of websites are the type of website (SNS vs. UGC), its scope (national

[4] WP29 is a working party established under art. 29 of the EU personal data protection directive, consisting of representatives of the supervisory authorities of EU member states, that may issue opinions and recommendations regarding the directive.

[5] http://www.oecd.org/dataoecd/57/14/38393115.pdf, p. 4.

vs. international), its target group (general vs. specific) and its purpose (business vs. private). The selection below includes websites on all these dimensions, i.e., websites that focus on user profiles (such as LinkedIn and Facebook) and websites that focus on content sharing (such as Wikipedia and YouTube). Both national and international websites are included (Hyves and Relatieplanet are typically Dutch sites). With regard to national sites, we chose Dutch sites for easy access. Some websites focus on the business sphere (e.g., LinkedIn), whereas others focus on the private sphere (e.g., Facebook). Some websites have a general audience (such as Wikipedia), whereas others target a very specific audience (Habbo and Hyves are aimed at youth, Relatieplanet aims at dating). We realize that within the framework of these criteria there are more websites to choose from (e.g., Facebook vs. Google+). In each category we chose to analyse the site with the largest number of users at the time of the research[6], maximizing the largest number of people affected by these privacy policies. It should also be noted that Wikipedia is not a commercial website and does not have an advertising revenue scheme or paid membership like the other websites selected. Although we realize this may entail different evaluation criteria, we decided to include Wikipedia as a typical example of a UGC site without user profiles that are visible for other users.

Despite the large numbers of users of these websites, we realize that analysing the privacy policies of only eight websites may not provide results that can be generalized for all UGC and SNS websites. Nevertheless, we think it may provide interesting indications of the way privacy policies are shaped by data controllers and used by data subjects.

Table 2: Analysis of the privacy policies of eight social media

[6] Note that Hyves has canceled its social network services in 2013.

	LinkedIn	YouTube	Relatieplanet	Habbo	Hyves	Twitter	Facebook	Wikipedia
C1.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
C1.2	Yes	Yes	Yes	Yes	No	Yes	No	No
C1.3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
C2.1	Yes	Yes	Yes	Yes	Yes/No	Yes	Yes	No
C2.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
C2.3	Yes	Yes	Yes	No	Yes	Yes	Yes	No
C2.4	Yes	Yes	Yes	Yes	Yes	No	No	Yes
C2.5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
C3.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C3.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C3.3	Yes	Yes	Yes	Yes	Yes/No	No	Yes/No	No
C3.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C3.5	Yes	Yes	Yes	Yes	No	No	No	No
C4.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes/No	Yes
C4.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes/No	Yes
C4.3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C4.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

For all eight websites, it was checked whether the criteria in Table 1 were *mentioned* in the website's privacy policy or user agreement. In Table 2 it is shown which criteria are mentioned. Table 2 does not reflect whether the criteria for consent are actually met or to what extent the criteria were met. For instance, if a privacy policy does not mention any user rights, criterion 3.5 is indicated 'no'. If anything on security measures is mentioned in the privacy policy or the user agreement, then criterion 3.3 is indicated 'yes'. Note that this does not mean that user rights are not complied with or all necessary security measures are in place. It just means that these issues are addressed. It may well be that a privacy policy indicates that no security measures are taken at all. This results in 'yes' because this is information that users may need to make a well-considered decision regarding their consent.

In short, if a website has taken all criteria into account, it means they have a sound and complete privacy policy (from a legal perspective), although this does not imply that the privacy policy is also fair (from an ethical perspective). Users may disagree with some of the terms and conditions, but when everything is addressed, they were enabled to make a well-considered decisions.

Also, it should be mentioned that the focus here is on what is stated in the privacy policies (i.e., the text documents provided), not on how the privacy policies are actually implemented in the technology and the data processing. Hence, the websites are examined on what is stated, which is clearly something different from the way the privacy policies are actually controlled and enforced.

From this overview, it becomes clear that most of the websites analysed actually do pay attention to most criteria for consent in their privacy policies (Table 2 contains considerably more ‘yes’ than ‘no’). It also becomes clear that many websites (4 out of 8) pay attention to all criteria for consent in their privacy policies (columns completely or almost completely filled with ‘yes’ for LinkedIn, YouTube, Habbo and Relatieplanet). Some websites pay attention to most criteria (Facebook, Hyves and Twitter) and only one website (Wikipedia) pays attention to only a limited set of criteria.

The privacy policies of Wikipedia and Facebook offer most room for improvement, These privacy policies do not meet all criteria for consent and, as such, consent may be considered flawed. In the case of Wikipedia, the need for an extensive privacy policy is debatable, since Wikipedia does not collect large amounts of personal data. At the same time, it is obvious that there is room for improvement of Wikipedia’s privacy policy. It could address obvious questions, like how minors are dealt with, making consent more explicit by ticking a box that you agree with and comply to the privacy statement when registering as a user, limiting the list of purposes for which data is collected, providing clarity on security measures that are taken and informing users about their rights (including the creation of the right to have accounts removed if users ask for this).

In the case of Facebook there is definitely room for improvement in the informed consent process. The Data Use Policy is very lengthy with 9500 words and takes more than one hour to read. Although, Facebook’s privacy policy is quite transparent (presentation, language, explanations) on what personal information is used and how by providing users with everyday language and clear examples, to see through the complete picture of data sharing may be more complicated for users. The reasons for this are (1) that relevant information is distributed over various documents and (2) that more parties than Facebook may be involved in using data on Facebook. Although (technical) security is mentioned in Facebook’s Data Use Policy, not reflecting in more detail on how security is guaranteed is a clear omission. However, Facebook provides extensive information (Twitter rules and policies) on how to stay safe on Facebook and explicitly warns users about the publicness of their data.

When looking at the criteria, it becomes clear that some criteria are no issue at all, such as C3.1 (which data), C3.2 (which purposes), C3.4 (accountability), C4.3 (reliability) and C4.4 (accessibility). These rows are completely filled with ‘yes’. Criteria C2.5 (up to date), C4.1 (specificity) and C4.2 (understandability) are also hardly an issue. In general, it becomes clear that all websites are doing a good job on how they are providing information. The information provided seems to be specific, detailed, understandable, reliable, accurate and accessible. We note, however, that even when a privacy policy is very understandable, this does not imply a user will also understand how personal data is processed.

However, some other criteria cause more concern. These are C1.2 (capability), C3.3 (security measures) and C3.5 (user rights). These are the criteria where there is room for improvement: these criteria may deserve more attention in privacy policies. But before starting a discussion on this, let us first consider what users expect from these and other criteria.

4. USER EXPECTATIONS

Based on the results of an extensive online survey (Brockdorff, 2012) and in-depth interviews with social media users (Manolea, 2012) which were carried out in 13 countries of the EU as part of the CONSENT project, and additional literature, we analysed which of the criteria in Table 1 are important to users. The survey used in this section was part of a EU-funded research project called CONSENT, set up by one of the key partners in the research project, the University of Malta, and translated and disseminated by the 19 partners in the research consortium. The questionnaire used in this study consisted of 75 questions and subquestions, covering general internet usage, online behaviour, particularly regarding online shopping and UGCs, and the related consumer perceptions and attitudes. Attitudes and practices in the disclosure of personal data and online privacy in social media use were particularly addressed. The questionnaire was available online between July 2011 and December 2011. A total of 8621 respondents from 26 countries completed at least a part of the questionnaire. It was possible for respondents to choose not to respond to all questions in the online questionnaire. Thus, the number of respondents to different questions can vary in the results reported in this paper. Percentages reported below are based on the number of respondents to that question, except for questions that allowed or required more than one answer, in which cases the number of responses was used rather (than the number of respondents).

Of the total number of respondents, 45% were male and 55% female. The average age of the respondents was 30 years. The highest level of education was 34% secondary school or lower and 66% tertiary education. 45% of the respondents were students. 71% of the respondents described their location as urban, 13% as suburban and 16% as rural. This quantitative analysis does not claim to be representative of the entire EU population, since the sample used was a non-probability sample: the questionnaire was online (excluding people without internet access) and the dissemination, though targeted at wider public to include all age groups, education levels and geographic locations, originated from the partners in the project, many of which are universities. This has resulted in a sample that is more likely to be representative of experienced internet users. Note that there are also cultural differences in privacy expectations among European countries. US-based research has shown that race and ethnicity play an influential role in how people use social media and share personal information (Correa and Jeong, 2011). Contextualizing cultural differences and reporting on the impact of cultural differences on the perception of privacy by SNS and UGC users was also part of the EU-project, but beyond the scope of this paper. For further background of the survey, including its set-up, the number and composition of respondents and the reliability of the results, we refer to the project's website: www.consent.law.muni.cz.

The survey had a more general focus on awareness, values and attitudes regarding privacy in social media use rather than a specific focus on the role of informed consent in social media use. Hence, the respondent internet users were not explicitly asked how important they considered each of the criteria for consent analysed in this paper. Nevertheless, the survey results do provide a number of indications how important internet users consider several aspects of consent to be, such as awareness and understanding of the personal data collected, the purposes for which the collected data are used and what social media users think of privacy policies. In order to deal with these limitations of our survey, we also used the results of the Eurobarometer Survey (2011) on attitudes on data protection and electronic identity in the EU for criteria that were not explicitly included in our own survey and to compare both surveys in cases where similar questions were asked. In this section, we will discuss user expectations regarding each of these criteria.

The criteria regarding the person who consents seem to be more important to data controllers than to data subjects, as they may indicate whether users are authorized and committed and whether accepted user agreements are legally binding. These criteria may be considered as a hindrance by some users, as they may be excluded from UGC and SNS services. This is most apparent for age (C1.1). It is a commonly accepted statement that particularly SNS services are something 'for the youngest generation'. According to research carried out within the EU Kids Online project, 59% of 9-16 year olds have a social networking profile (Livingstone et al., 2011). From the perspective of minors, it is fair to state that social media are, in general, important to them. The Eurobarometer survey 359 (2011) found that “around 94% of the 15-24 are using the Internet (EU 66%). 84% of them are using social networking sites (EU 52%) and 73% of them are using websites to share pictures, videos, movies (EU 44%)”. According to another recent study, 44% of teens have even lied about how old they are online to access sites with age restrictions (Fox, 2011). This suggests that these teens are younger than the ages for which the sites are eligible. Note that, apart from getting access to particular websites, minors may have other reasons for lying about their age, such as their reputation among peers. Although there seems to be a widespread assumption that youth do not care about privacy issues when online, this is challenged by research results (boyd and Hargittai, 2010). Younger people also seem to change privacy settings more often than older people (Madden and Smith, 2010).

With regard to the capability (C1.2) and competence (C1.3) of users to consent, the majority of the respondents of our survey who read privacy policies indicated they completely understand (21%) the privacy policy or at least understand most parts (42%), see Figure 4. Note that these figures refer only to respondents who indicated to read privacy statements, not to all respondents. At the same time, the survey revealed that most respondents never (27%), rarely (27%) or sometimes (23%) read the privacy policies, see Figure 3A. Hence, most internet users in the survey did not read privacy policies, but a comparably large portion of those who claim that they do read privacy policies show confidence that they understand these policies. Note that this survey question included all internet users, not merely UGC or SNS website users. Hence, respondents also include people who do not use UGC or SNS website, but do use the internet, such as people who only have an email account. Also note that this contrasts with the Eurobarometer survey (2011), which found that 58 % of European Internet users read privacy policies. Other research, however, confirms that privacy policies are rarely read by users (Arcand et al., 2007, Beldad, 2011, Bolchini et al., 2004, Graf et al., 2010, Jensen and Potts, 2004, Lichtenstein et al., 2003, Milne and Culnan, 2004, Pan and Zinkhan, 2006, Sheehan, 2005). Finally, it should be mentioned that the fact that users feel capable of understanding (see also C4.1) the privacy policies does not imply that they do actually understand the privacy policies. From the survey results, it cannot be determined whether users actually understand the privacy policies, since many respondents only read the privacy polices sometimes, rarely or never at all.

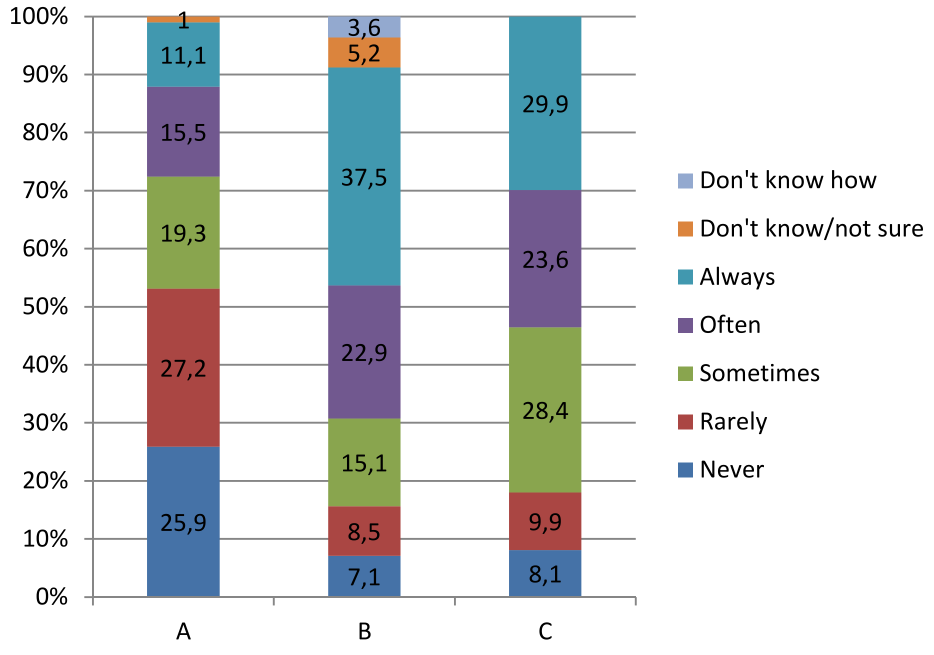

Figure 3: (A) When you create an account with a website you have not used before do you read that website's privacy statement or policy? (n=7057).(B) Do you watch for ways to control what people send you online (such as check boxes that allow you to opt-in or opt-out of certain offers? (n=6637). (C) Have you ever changed any of the privacy settings of your personal profile on a UGC site? (n=6770).

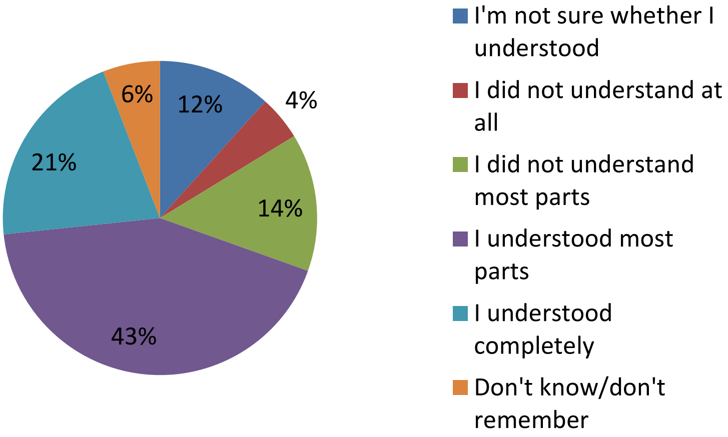

Figure 4: When you have read privacy statements or privacy policies you would say that? (n=5124)

Most respondents (75%) sometimes, often or always watch for ways to control what they are sent online (such as check boxes that allow opt-in or opt-out of certain offers), see Figure 3B. Hence, it may be concluded that people consider such controls important. This may also indicate that users think written consent (C2.1) is important and that the extent of their consent is important (full or partial consent, C2.2). This is confirmed by another survey question, showing that that 82% of the respondents sometimes, often or always change their privacy settings, when there are options available for personalizing your privacy settings, see Figure 3C. It may be expected that more options for privacy settings will become an increasingly important topic in social media (McAllister, 2012). However, despite users adopting strategizing behaviours, their levels of protective skills may be limited (Acquisti and Grosslags, 2005, LaRose and Rifon, 2007, Metzger, 2004). Research indicated that younger SNS users change privacy settings more often than older SNS users (Madden and Smith, 2010). Still, it is unknown whether users understand the changes they make in their privacy settings and to which extent these changes meet their preferences Although the survey results cannot confirm this, there seems to be an increase in the number of users regularly changing privacy policies. For instance, an internet study in 1991 (Mackay, 1991) showed that users rarely change default settings, whereas a Facebook study in 2010 showed that most users report having modified their privacy settings at least once a year (boyd and Hargittai, 2010).

In addition to low rates of privacy policy reading, as mentioned above, most respondents (73%) also indicated that they never, rarely or sometimes read the terms and conditions before accepting them. When users do not read the privacy policy and the terms and conditions, they probably do not know what they consent to. As a result, their consent is unlikely to be strong consent (C2.3) and up to date (C2.5). Whether their consent is an independent decision (C2.4), is difficult to answer, since the qualitative interview results suggest that users have a rather ambivalent relationship to UGC websites. Many users appear to sign up for accounts due to certain forms of peer pressure, but after an initial phase become low-frequency users. It might be argued that the extent to which people would miss a particular website indicates their dependency on this website. Although we note that there is no research available on the link between not missing a particular website and the independency of consent decisions using the website, most users indicate they would not really miss a particular site if it were to close down. Only Facebook (by 59%), Twitter (by 28%) and LinkedIn (by 6%) will be missed by users. Other websites are not missed (< 3%).

Users show concern for privacy, although there seems to be an incongruity between public opinion and public behaviour: people tend to express concern about privacy, but when asked about it, they routinely disclose personal information because of convenience, discounts, and other incentives, or a lack of understanding of the consequences (Regan, 2002). These tensions between attitudes and practices were also found by Acquisti and Gross (2006). As there may be longer periods of time between the data collection and actions based upon the processing or sharing of such information, the connection between the collected data and the resulting decisions may not always be transparent for data subjects. For instance, when the information collected is used for profiling, such profiling techniques, by their nature, tend not to be visible processes for data subjects (Bygrave, 2002, Custers, 2004). The fact that users are concerned about their privacy is also confirmed by the survey results, in which internet users indicated on a 7-point Likert scale that there is a high potential for privacy loss associated with giving personal information to websites (mean 5.78, sd 1.43), and that privacy is the most important thing to keep when online (mean 5.28, sd 1.59).

Respondents clearly indicated which types of data they disclosed (C3.1) – results largely in line with the Eurobarometer survey – and indicated they were aware of the purposes for which data controllers can and may collect, use and share personal data of users (C3.2). An overview is shown in Figure 5. Most respondents (74%) indicated they were aware that account or profile information may be used by the website owners for a number of purposes. In terms of actual uses by website owners of account and profile information most respondents were aware that this information can be used to customize the content a user sees (72%), to customize the advertising a user sees (79%), and to contact users by email (87%). There was also awareness, though less so, of other less publicized practices relating to the use of account and profile information; 61% were aware that information about user behaviour (not linked to the user’s name) can be shared within the website owner’s company; 61% were aware that this information (linked to the user’s name) can be shared within the website owner’s company; and 54% were aware that such information (not linked to the user’s name) can be sold to other companies.

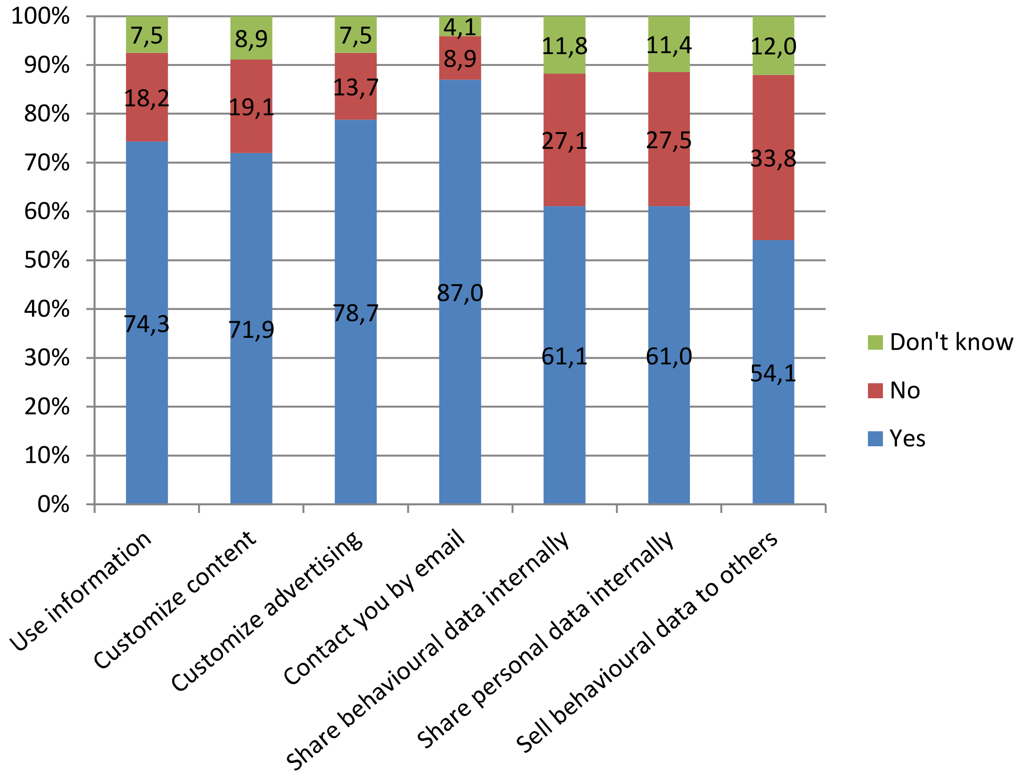

Figure 5: The information you include in your account or profile on a website may be used by the website owners for a number of purposes. Were you aware of this? Note that the behavioural information consists of data not linked to the individual user.

Regarding concerns for security measures (C3.3), the survey results show that the respondents' attitudes towards online technical protection measures are mostly in line with their awareness levels, with the exception of Ireland and the UK. The portion of respondents applying various security measures was on average clearly above 50% and in some countries up to 90%. At the same time, the survey results showed that only a minority of UGC/SNS users think it is likely or very likely that their personal safety is put at risk by putting personal information on these websites. Similarly, only a minority thinks it is likely or very likely that they will become a victim of fraud, will be discriminated against or suffer reputation damage. This is shown in Figure 6. These results are in line with Park (2011) who found low levels of understanding of surveillance practices among internet users. The figures allow for the conclusion that many of them use their technical knowledge to specifically protect themselves against physical or material risks – and, thus, do not show too much concern in this respect. Note that even though users may adopt strategizing behaviours, their levels of protective skills may be very limited (Acquisti and Grosslags, 2005). This hypothesis is supported by the fact that users easily share lots of information (see C3.1 above). Note that users may overestimate the quality of their security measures. For instance, users often choose easy-to-remember passwords, which are usually easy to breach (Schneier, 2000). For teens this is probably even worse, as nearly one-third (30%) of teens have shared a password with a friend (Fox, 2011).

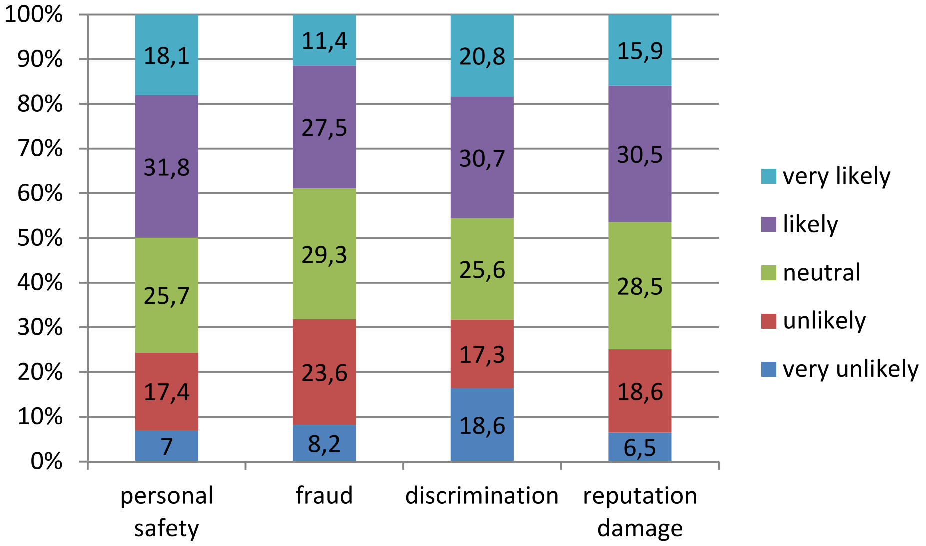

Figure 6: For each of these situations please indicate how likely you think that this could happen as a result of your putting personal information on UGC sites: your personal safety being at risk (n=6535), you becoming victim of fraud (n=6550), you being discriminated against (n=6525) and your reputation being damaged (n=6520).

With regard to accountability of data controllers (C3.4), users want to know their reputation in order to decide whether to trust them (Solove, 2007). However, trust in (online) companies is limited. According to the Eurobarometer survey (2011), 70% of European citizens are concerned about how companies use their data; they trust public authorities better than companies, including online social networks and other Internet companies.

For user rights (C3.5), this is different, however. As indicated above, 72% of the respondents never, rarely or sometimes read the terms and conditions before accepting them. This indicated that users may not be well informed about their rights. This hypothesis is confirmed in other research, showing that users are not always aware (enough) of their rights and obligations with respect to sharing (personal) data (Van den Berg and Van der Hof, 2012). Note that users may also have access to other sources than the terms and conditions of a website to inform themselves about their rights, such as consumer protection websites or the media. It can be questioned, however, whether such (more general) sources can fully substitute the reading of (more specific) terms and conditions of a particular website. The conclusion that users don't care much about the rights they can exercise may seem to contradict the findings from many studies that citizens place a high value on their right to privacy (Hallinan et al., 2012). A possible explanation for this contradiction may be that users are often unaware of, or not well informed about, the rights they have, making it difficult for them to 'match' the privacy policies and terms and conditions with the rights they have under the Data Protection Directive. Another explanation may be that users simply trust that social network sites have the necessary mechanisms in place for users to exercise their rights, or trust that the regulator will step in if their rights are violated. The qualitative interview results showed indications that not-reading among interviewees was often based on a perception that prevailing offline conditions of perceived general social 'law and order' could be assigned to the online environment. Other frequent reasons for not-reading were either the concept of privacy itself being underdeveloped or a perceived helplessness which was often masked as disinterest in online privacy issues. Another strong reason given for not-reading was the perception that privacy policies primarily serve the purpose of protecting the website owners rather than the website users.

The reasons for not reading privacy policies are shown in Figure 7. Most people do not read privacy statements because they consider them too long to read (55.7%) or too difficult to understand (8.7%). 7.4% of the users who never reads privacy policies do not care about privacy policies and 6.8% indicates that websites will ignore their policies anyway. Others indicated not to know about privacy policies, not have anything to hide or not to know where to find privacy policies. These data suggest that, while citizens value their right to privacy highly, they do not attach the same importance to the actual exercising of their rights.

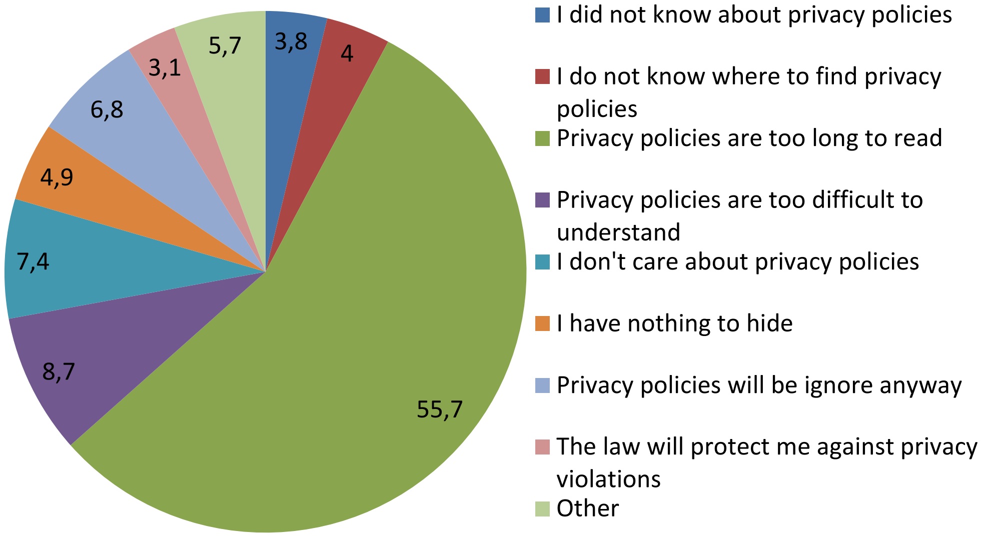

Figure 7: Why don't you ever read privacy policies? Percentages. (n=1875)

The level of detail in the privacy policies (C4.1) is a concern for most users. The fact that users consider the privacy policies too long and too detailed is confirmed by other research, showing that users of social network sites do not want to spend a lot of time reading privacy policies, on average 1-5 minutes (Van den Berg and Van der Hof, 2012). However, most websites we analysed (see previous section) provide texts that are much longer, often taking half an hour to read and sometimes even taking more than one hour to read.

Users think the information provided for their consent decisions (C4.2) is understandable. As mentioned above, 64% of the survey respondents indicated they understand the information completely or at least most parts of them. Only 5% indicated they do not understand the information at all. Of the people who do not read privacy statements, merely 9% indicated they do not read privacy statements because they are too difficult to understand. In the Eurobarometer (2011, p. 112) a quarter of those who read privacy statements said they do not fully understand them. Another indication that most users believe they understand privacy issues is the fact that, when asked why they have never changed the privacy settings, only 12% indicated that they do not know how to change the privacy settings. Note that users may be too confident that they understand everything. A large number of interviewees in the qualitative research claimed that they found the language used in privacy policies difficult to understand, but those interviewees who did read privacy policies stated that they viewed the reading 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. However, even those readers expressed their difficulties in the "learning process".

The survey did not ask whether users considered the information provided reliable and accurate (C4.3). However, as indicated above, users want to know the reputation of others in order to decide whether to trust them and, therefore, reliable and accurate information is important to them. Note that, currently, trust in online companies is limited (Eurobarometer, 2011, p. 137).

With regard to accessibility of the information provided, of the 26% of the respondents indicating that they never read the privacy policies, only 4% did not know where to find privacy policies on a website, see Figure 7. Similar patterns can be seen with other information, such as changing the privacy settings. Most people indicated that they change privacy settings. Of the people who have never changed the privacy settings (8% of the respondents), 10% indicated that they do not know that privacy settings existed and 11% indicates that they did not know that they could change the privacy settings. Hence, we conclude that most people know where to find this information.

A more general survey finding is that users seem to be often dissatisfied by privacy policies of UGC websites. When asked “have you ever decided to not start using a website or to stop using a website because you were dissatisfied with the site’s privacy policy”, 47.2% answered “yes”, 30.5% answered “no” and 22.3% indicated “don’t know” (n=4728). Note that among the respondents who answered “no”, there may be people who are dissatisfied with a privacy policy who nevertheless start or continue using that website. Whereas the previously mentioned low levels of users reading privacy policies indicate little interest of users in privacy policies, these results seem to go one step further as they seem to indicate rather low levels of acceptance and significant dissatisfaction with current practices and policies.

5. COMPARE AND CONTRAST ANALYSIS

In Table 3 the current practices (the analysis of privacy policies discussed in Section 3) are compared with the users expectations (discussed in Section 4). The information in Table 2 is condensed by counting the number of times that a criterion is taken into account in the privacy policies analysed. One to three times ‘Yes’ is considered rarely, four or five times is considered sometimes, six to eight times is considered often.

When these results are compared, it immediately draws attention that there is a lot of correspondence between the privacy policies and the user expectations. Many of the criteria are taken into account often in the privacy policies and are important to users. The criteria that are sometimes, but not always, taken into account are at the same time less important to users. Hence, for the largest part, the current practices do correspond with the user expectations. One criterion is taken into account in the privacy policies but is not considered important by users. This criterion (C4.1: is it clear which rights can be exercised? Is it clear how these rights can be exercised?) may thus be considered as more or less superfluous or as an extra. Another criterion is considered important to users (C3.5: is the information provided specific and sufficiently detailed?) but not taken into account in the privacy policies and, thus, requires further attention.

Table 3: Comparison of current privacy practices and user expectations

	In privacy policies?	Important to users?	Does this correspond?

C1.1	Often	Yes	Yes
C1.2	Sometimes	N/A	N/A
C1.3	Often	N/A	N/A
C2.1	Often	Yes	Yes
C2.2	Often	Yes	Yes
C2.3	Often	Yes	Yes
C2.4	Often	Yes	Yes
C2.5	Often	N/A	N/A
C3.1	Often	Yes	Yes
C3.2	Often	Yes	Yes
C3.3	Sometimes	No	Yes
C3.4	Often	Yes	Yes
C3.5	Sometimes	Yes	No
C4.1	Often	No	No
C4.2	Often	Yes	Yes
C4.3	Often	Yes	Yes
C4.4	Often	Yes	Yes

Note that these results are in line with other research results, in which surveys revealed that the kinds of information respondents say they would like to receive align neatly with the kinds of information data controllers are required to communicate as stipulated in data protection law (Van den Berg and Van der Hof, 2012). Not all criteria analysed in this research are backed by legal provisions. For instance, there are no legal obligations in the existing EU data protection law regarding the person who consents (C1.1-C1.3), up to date consent (C2.5), understandability (C4.2) and accessibility (C4.4). Written consent as such is not mentioned in EU data protection law as a legal requirement but there is the (technologically more neutral) legal requirement of explicit consent. Some of these issues are regulated in national legislation to some extent, however, such as in civil codes (C1.1-C1.3), or in other legal documents, such as the opinions of the Article 29 Working Party, an advisory body to the European Commission on data protection issues (C4.2 and C4.4). The proposal for a General data protection regulation addresses most of these issues though. Article 11 of the proposal requires data controllers to present data subjects with transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

An important shortcoming in the comparison shown in Table 3 is that the privacy policies were assessed on the mentioning of the criteria for consent, whereas expectations of users may be influenced not only by the mentioning of these criteria in privacy policies, but also by the contents of these privacy policies, i.e., by the ways these criteria are dealt with. For instance, a privacy policy mentioning that parental consent for minors is not required means that this criterion is addressed, but it also implies that this criterion is not fulfilled. Users who disagree with this may find this criterion more important accordingly. An elaborate analysis of why a particular criterion is or is not important to users is beyond the scope of this research.

We also recognize that the binary approach (yes/no) in presenting the user expectations does not reflect more nuanced views that users may have on each of the criteria (Litt and Hargittai, 2014). Users may consider some criteria important depending on the context, which is beyond the scope of this research. Also, users may have expectations somewhere halfway (e.g., ‘a little important’ or ‘rather important’) or even beyond the spectrum (e.g., ‘very important’ or ‘extremely important’). These qualifications were to some extent discussed in the previous section, but are not shown in Table 3. We feel the data do not allow for making more detailed statements on the extent to which users consider the criteria important. Hence, Table 3 only provides indications and should not be regarded as a statistical result.

In summary, all criteria that are important to users are taken into account by most privacy policies, and most criteria taken into account by (most) privacy policies are also important to users. For the largest part, current privacy practices correspond to user expectations. Only some criteria may either require further research (i.e., users’ attitudes towards competence to consent and up to date consent) or, regarding the criterion of specific and sufficiently detailed information, it can be questioned whether data controllers put in too much effort, as these criteria are often taken into account in privacy policies but considered of little importance by users. On the one hand, it may be argued that these criteria may be in the interest of data controllers, as they may consider it important that their users are authorized and committed. On the other hand, in case of a dispute, it may be more important for data controllers to be able to show they provided all necessary information than to ensure that users have read and understood all information provided. As a result, data controllers may be inclined to put lengthy privacy policies on their websites to cover all legal aspects, rather than brief privacy policies in everyday language. When privacy policies are only put on websites as a formality, however, they may not achieve the intended goal of properly informing users in order to make well-considered decisions regarding consent. They may lack clarity about which user rights can be exercised and how (criterion C3.5) and, as a result, the reality of privacy policies and user expectations drift apart.

As far as implications for EU policy is concerned, we think these tensions between the legal approach (legislation and privacy policies) and practice (user’s attitudes, behaviour and expectations) should have much more focus. Even though current EU personal data protection legislation is under revision, we see that the proposed legislation again heavily focuses on the existing views of autonomous, highly rational and well-informed data subjects. We doubt whether this really reflects the needs, interests and preferences of internet users.

6. CONCLUSIONS

In this research, we analysed the current practices of social media by analysing the privacy policies and user agreements of a selection of eight SNSs and UGCs. Despite the large numbers of users of these eight websites, we realize that analysing the privacy policies of only eight websites may not provide results that can be generalized for all UGC and SNS websites. Nevertheless, our analysis revealed that most of the websites analysed have privacy policies that take most relevant criteria for consent into account. As such, it may be argued that, even though there is no legal obligation to have a privacy policy at all, most of the websites analysed do have sound privacy policies in which they regulate the process of informed consent. Some websites regulate parts of the consent process in their terms and conditions or in their user agreements, rather than in their privacy policy, which may reduce the accessibility and understandability to some extent. All this does not imply, however, that the privacy policies are always fair and users may disagree with the terms and conditions, but most issues are addressed, including all issues that users consider important.

Some websites can further improve their privacy policies. The privacy policies of Wikipedia and Facebook offer most room for improvement. These privacy policies do not meet several criteria for consent and, as such, consent may be considered flawed. In the case of Wikipedia, the need for an extensive privacy policy is debatable, since Wikipedia does not collect large amounts of personal data. Nevertheless, it could address obvious questions, like how minors are dealt with, making consent more explicit by ticking a box that you agree with and comply to the privacy statement when registering as a user, limiting the list of purposes for which data is collected, providing clarity on security measures that are taken and informing users about their rights (including the creation of the right to have accounts removed if users ask for this).

In the case of Facebook, a website that extensively collects and processes personal data, the need for improvement is more obvious. The Data Use Policy is very lengthy with 9500 words and takes more than one hour to read. Although, Facebook's privacy policy is quite transparent (presentation, language, explanations) on what personal information is used and how by providing users with everyday language and clear examples, to see through the complete picture of data sharing may be more complicated for users. The reasons for this are (1) that relevant information is distributed over various documents and (2) that more parties than Facebook may be involved in using data on Facebook. Although (technical) security is mentioned in Facebook's Data Use Policy, not reflecting in more detail on how security is guaranteed is a clear omission. However, Facebook provides extensive information (Twitter rules and policies) on how to stay safe on Facebook and explicitly warns users about the publicness of their data.

Furthermore, we analysed user expectations based on a survey on the consumer behaviour of UGC users and their needs, preferences and interests. This analysis showed that consumers place high value on privacy, but also that users show little interest in reading privacy policies. There is still little known about users' interest in criteria for consent that they consider to be the responsibility of (or in the interest of) data controllers, including, for instance, whether consent is authorized (C1.2-C1.3) and whether consent is up to date (C2.5) – see Table 3. Furthermore, the perceived physical or material risk of sharing or disclosing personal data via UGC websites (particularly regarding personal safety, fraud, discrimination and reputation damage) is low (see Figure 6).

When the current practices and the user expectations are compared with each other, it becomes clear that most websites have privacy policies that take most relevant criteria for consent into account, including most issues that users consider important. Some criteria are not taken into account, but these criteria appear to be of little or no importance to users – except for the clearness of user rights. Only for some criteria (i.e., competence to consent, up to date consent and specific and sufficiently detailed information) it can be questioned whether data controllers put in too much effort, as these criteria are often taken into account in privacy policies but considered of little importance by users.

The survey findings show that social media users (generally speaking) do not read privacy policies and show low levels of acceptance and significant dissatisfaction with current practices and policies. There appears to be a large disconnection between users and data controllers. Data controllers appear to focus mainly on complying with all existing legislation rather than on the needs, interests and preferences of users. On the one hand this may be expected as compliance is important for data controllers in order to avoid sanctions and to build a solid reputation and gain trust among users. On the other hand, when it comes to reputation and trust, it may also be argued that carefully listening to the needs, interests and preferences of users is also important – something that may go further than drafting long and detailed privacy policies. Instead, more focus of social media on building trust among users when it comes to their ways of collecting and processing personal data may be the way forward, for instance, by creating more transparency and responsible use of their personal data on social media by users, particularly minors.

7. REFERENCES

Adjerid, I., Acquisti, A., Brandimarte, L., Loewenstein, G. (2013), *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency*, in: SOUPS '13 Proceedings of the Ninth Symposium on Usable Privacy and Security, Article No. 9.

Acquisti, A., and Grosslags, J. (2005) Privacy and rationality in decision making, *IEEE Security and Privacy*, 3 (1), 26-33.

Acquisti, A., and Goss, R. (2006) Imagined communities: Awareness, information sharing and privacy on Facebook. PET Workshop, see: www.heinz.emu.edu.

Acquisti, A. (2009), Nudging Privacy: the Behavioral Economics of Personal Information, in: *Security & Privacy Economics*, November/December 2009.

Arcand, M., Nantel, J., Arles–Dufour, M., and Vincent, A. (2007) The impact of reading a Web site's privacy statement on perceived control over privacy and perceived trust, *Online Information Review*, volume 31, number 5, pp. 661–681.

Beldad, A. (2011) *Trust and information privacy concerns in electronic government*. Enschede: University of Twente.

Böhme, R., Köpsell, S. (2010), Trained to accept?: a field experiment on consent dialogs, in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2403-2406.

Bolchini, D., He, Q., Anton, A., and Stufflebeam, W. (2004) I need it now: Improving website usability by contextualizing privacy policies. In: N. Koch, P. Fraternali and M. Wirsing (editors). ICWE 2004. *Lecture Notes in Computer Science*, volume 3140. Heidelberg: Springer, pp. 31–44.

boyd, D., and Hargittai, E. (2010) Facebook Privacy Settings: Who Cares? First Monday, 15 (8), pp. 23.

Brockdorff, N. (2012) *Quantitative measurement of end-user attitudes towards privacy*, Work Package 7 of Consent. http://www.consent.law.muni.cz/

Bygrave, L.A. (2002) Data *protection law; approaching its rationale, logic and limits*, Information law series 10, The Hague, London, New York: Kluwer Law International.

Correa, T., and Jeong, S.H. (2011) Race and online content creation, *Information, Communication and Society*, 14, p. 638-659.

Custers, B.H.M. (2004) The Power of Knowledge; Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology, Tilburg: Wolf Legal Publishers.

Custers, B.H.M., Schermer, B. and Van der Hof, S. (2013) *User Expectations Regarding Social Media Privacy Statements.* In: proceedings of the Annual Conference on Management and Social Sciences, April 16-18th 2013, Bangkok, Thailand.

Custers, B.H.M., Van der Hof, S., Schermer, B., Appleby-Arnold, S., and Brockdorff, N. (2013) Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law, *SCRIPTed, Journal of Law, Technology and Society*, Volume 10, Issue 4, p. 435-457.

Eurobarometer Survey 359 (2011) *Attitudes on Data Protection and Electronic Identity in the European Union*, Brussels, June 2011

Fox, Z. (2011) *Nearly Half of Teen Internet Users Have Lied About Their Age*. http://mashable.com/2011/12/13/teens-social-media/

Goffman, E. (1959) *The Presentation of Self in Everyday Life*, New York: Anchor Books.

Gold, E.B. (1996) Confidentiality and Privacy Protection in Epidemiologic Research, In:

Ethics and epidemiology, S.S. Coughlin and T.L. Beauchamp (eds.) New York/Oxford: Oxford University Press.

Graf, C., Wolkerstorfer, P., Kristjansdottir, K., and Tscheligi, M. (2010) *What is your privacy preference? An insight into users' understanding of privacy terms*, paper presented at NordiCHI2010 (Reykjavik, Iceland, 16–20 October 2010).

Hallinan, D., Friedewald, M., McCarthy, P. (2012), Citizens' Perceptions of Data Protection and Privacy, *Computer Law and Security Review*, Vol. 28, No. 3, 2012, pp. 263-272.

Hargittai, E., and Litt, E. (2013) New Strategies for Employment? Internet Skills and Online Privacy Practices during People's Job Search, *IEEE Security & Privacy*, Vol. 11, No 3, p. 38-45.

Hornung, G. (2012) A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012, *SCRIPTed*, Vol. 9, No. 1, April 2012.

Kuner, Chr. (2012) The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, *Privacy and Security Law Report*, February 6th 2012.

Krügel, T. (2010) *Identifying and classifying UGC services*, Deliverable 2.1 of Consent.

Jensen, C., and Potts, C. (2004) *Privacy policies as decision–making tools: An evaluation of online privacy notices*, CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 471–478.

LaRose, R., and Rifon, N. (2007) Promoting i-safety: effects of privacy seals on risk assessment and online privacy behaviour, *Journal of Consumer Affairs*, 41 (1), 127-149.

Lichtenstein, S., Swatman, P., and Babu, K. (2003) *Adding value to online privacy for consumers: Remedying deficiencies in online privacy policies with an holistic approach*, Proceedings of the 37th Annual Hawaii International Conference on System Sciences, pp. 1–10, and at http://dro.deakin.edu.au/view/DU:30005153.

Litt, E. (2012) Knock, Knock. Who's There? The Imagined Audience, *Journal of Broadcasting & Electronic Media*, Vol. 56, no.3, p. 330-345.

Litt, E., and Hargittai, E. (2014) Smile, snap and share? A nuanced approach to privacy and online photo-sharing, *Poetics*, 42 (2014), pp. 21.

Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children*. LSE, London: EU Kids Online.

Madden, M., and Smith, A. (2010) Reputation management and social media, *Pew Internet & American Life Project*, www.pewinternet.org.

McCrystal, M., and Barnes, A. (2002) On-line consent to the disclosure of personal data: assessing rights and rituals. In: *The transformation of organisations in the information age; social and ethical implications*, Ethicomp 13-15 November 2002, I. Alvarez, T.W. Bynum, J.A. de Assis Lopez, S. Rogerson (eds.) Proceedings of the sixth international conference, Lisbon, Portugal: Universidade Lusiada.

Metzger, M.J. (2004) Exploring the barriers to electronic commerce: privacy, trust and disclosure online, *Journal of Computer-Mediated Communications*, Vol. 9, Issue 4.

Milne, G., and Culnan, M. (2004) Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices, *Journal of Interactive Marketing*, volume 18, number 3, pp. 15–29.

Mommers, L., & Kielman, H. (2010) *Analytical bibliography of existing privacy criteria*, Deliverable 9.1 of Consent. http://www.consent.law.muni.cz/

Mackay, W. (1991) Triggers and barriers to customizing software, *proceedings of the SIGCHI conference on human factors in computing systems*, New Orleans, p. 153-160.

Manolea, B. (2012) *Qualitative study of UGC users and UGC non-users attitudes towards privacy*, Work Package 8 of Consent. http://www.consent.law.muni.cz/

McAllister, N. (2012) Facebook's Zuckerberg awarded privacy patent, *The Register*, July

24th 2012, http://www.theregister.co.uk/2012/07/24/zuckerberg_privacy_patent/

Nazarek, W. (2012) *Impact of common policies and practices: legal requirements for obtaining consent*, Deliverable 6.1 of Consent. http://www.consent.law.muni.cz/

Nissenbaum, H. (2011) A Contextual Approach to Privacy Online, *Daedalus, Journal of the American Academy of Arts & Sciences*, 140 (4) Fall 2011, p. 32-48.

Pan, Y., and Zinkhan, M. (2006) Exploring the impact of online privacy disclosures on consumer trust, *Journal of Retailing*, volume 82, number 4, pp. 331–338.

Park, Y.J. (2011) Digital Literacy and Privacy Behavior Online, *Communications Research*, 40 (2), p. 215-236.

Pollach, I (2007), What's wrong with online privacy policies?, in: *Communications of the ACM*, volume 50, number 9, pp. 103–108.

Regan, P.M. (2002) *Privacy and commercial use of personal data: policy developments in the US*. Paper presented at the Rathenau Institute Privacy Conference, Jan. 17th 2002, Amsterdam.

Schermer, B.W., Custers, B.H.M., Van der Hof, S. (2014) The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection, *Ethics and Information Technology* [accepted March 2014].

Schneier, B. (2000) *Secrets and Lies; digital security in a networked world*, New York: Wiley Computer Publishing.

Sheehan, K. (2005) In poor health: An assessment of privacy policies at direct–to–consumer Web sites, *Journal of Public Policy Marketing*, volume 24, number 2, pp. 273–283.

Shultz, M.M. (1996) Legal and Ethical Considerations for Securing Consent to Epidemiologic Research in the United States, In: *Ethics and epidemiology*, S.S. Coughlin and T.L. Beauchamp (eds.) New York/Oxford: Oxford University Press.

Solove, D. (2007) *The Future of Reputation*, New Haven, CT, Yale University Press.

Solove, D. J. (2013), Privacy Self-management and the Consent Dilemma, in: *Harvard Law Review*, vol. 126, pp. 1880-1903

Toubiana, V., and Nissenbaum, H. (2011) An Analysis of Google Logs Retention Policies, *Journal of Privacy and Confidentiality*, Vol. 3, Issue 1, Article 2.

Turow, J. (2001) *Privacy policies on children's Web sites: Do they play by the rules?* at http://www.asc.upenn.edu/usr/jturow/release.html.

Turow, J., Feldman, L., and Meltzer, K. (2005) *Open to exploitation: American shoppers online and offline*, Report of the Annenberg Public Policy Center, University of Pennsylvania, Philadelphia.

Van den Berg, B. & Van der Hof, S. (2012) What happens to my data? A novel approach to informing users of data processing practices, *First Monday*, Vol. 17, No. 7, July 2nd 2012.

Westin, A. (1967) *Privacy and Freedom*. London: Bodley Head.