scripted

Volume 10, Issue 4, 2013

Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law

Bart Custers[*], *Simone van der Hof,*[**] *Bart Schermer,*[***]
Sandra Appleby-Arnold,[****] *Noellie Brockdorff*[****]

Abstract

In this paper, user expectations with regard to privacy and consent when using social media are compared with the EU legal framework for personal data protection. This analysis is based on a set of criteria for informed consent distilled from an analytical bibliography. User expectations regarding these criteria are derived from survey results. For each of the criteria for informed consent it is assessed whether there exists legal provisions in the existing EU personal data protection law and in the proposed legal framework in this area. A gap analysis between user expectations regarding each criterion and the availability or absence of related legal provisions shows that many but not all aspects of consent are addressed in both the current and the proposed legislation. Furthermore, the EU personal data protection legislation only provides a very general scope regarding consent and does not contain many details on what adequate consent procedures should look like. There is, at some points, a disconnect between the abstract legal provisions and the concrete practical implementations in the architecture and privacy statements of social media. Suggestions for solving these disconnects are made by suggesting changes at a practical level, by adjusting the legal framework, or both. Finally, the limits of the current models for personal data protection and consent are discussed.

DOI: 10.2966/scrip. 100413.435

[*] Research Manager, Faculty of Law, Leiden University.

[**] Professor, Faculty of Law, Leiden University.

[***] Assistant Professor, Faculty of Law, Leiden University.

[****] Department of Cognitive Science, University of Malta.

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[1], which was co-funded by the European Union under the Seventh Framework Programme. This project examined how consumer behaviour and commercial practices are changing the role of consent in the processing of personal data. Part of the project was 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, we examined the current practices of eight social media sites by analysing their privacy statements.[2] These results were compared and contrasted with user expectations regarding informed consent derived from survey results.

In this paper, a set of criteria for informed consent is assessed, focusing on the question of the extent to which there exist legal provisions both in the existing and in the proposed legal framework of EU personal data protection. A gap analysis is made between user expectations regarding each criterion and the availability or absence of related legal provisions in both the current and the proposed legislation. Where there is a disconnect between the legal provisions and the user expectations, practical changes or changes in the legal framework are suggested.

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, the user expectations for each of the criteria are analysed using survey results. In Section 4, an analysis is carried out on which legal provisions are present in both the existing and the proposed EU legal frameworks for data protection. In Section 5, a gap analysis is made between the legal framework and user expectations. Furthermore, practical changes and changes in the legal framework are suggested that may address any disconnects discovered in the gap analysis. In Section 6, the limits of the current models for personal data protection and consent are discussed. Finally, in Section 7, conclusions are provided.

---

[1] "CONSENT" available at <www.consent.law.muni.cz> (accessed 12 Dec 13).

[2] B Custers, B Schermer and S Van der Hof, "User Expectations Regarding Social Media Privacy Statements", (Annual Conference on Management and Social Sciences, Bangkok April 2013).

2. Criteria for Consent

The compare and contrast analyses of our research are based on a set of criteria for consent. These criteria are based on an analysis of a bibliography on existing privacy criteria,[3] an analysis of the concepts on which the existing legal obligations with regard to consent are based[4] 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).[5]

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 is thus able and enabled, to some extent, to assess 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, the condition is generally added that consent must be informed. In this paper, by consent we mean informed consent.

Table 1 presents the criteria that 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?).

---

[3] L Mommers and H Kielman "Analytical bibliography of existing privacy criteria, Deliverable 9.1 of Consent "(2013). available at http://www.consent.law.muni.cz (forthcoming).

[4] W Nazarek "Impact of common policies and practices: legal requirements for obtaining consent, Deliverable 6.1 of Consent" (2013) available at http://www.consent.law.muni.cz (forthcoming).

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

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 consent?
		C1.3	Is the person who consents competent to consent?
	Criteria on how to give consent	C2.1	Is the consent written?
		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 how well-considered the decision to consent was	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?

3. User Expectations

Based on the results of an extensive online survey[6] and in-depth interviews with internet users,[7] which were carried out in thirteen 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 our EU funded research project called CONSENT, which was set-up by the University of Malta (one of the key partners in the research project) and translated and disseminated by the nineteen partners in the research consortium. A snowball technique was used by the partners to distribute the links to the survey, which involved asking people to complete the survey and further distribute it. To promote the survey a combination of various dissemination channels were used including: press releases, mailing lists, newsletter, banners, articles in newspapers, journals (online and paper versions) and promotion on specific websites of public and private stakeholders such as on social media (e.g. creation of specific Facebook events or blogging) and personalised emails.

The survey was an online survey regarding the awareness, values and attitudes of social media users towards privacy. The survey was comprised of seventy-five

[6] N Brockdorff et al "Quantitative measurement of end-user attitudes towards privacy, Work Package 7 of Consent" (2013) available at http://www.consent.law.muni.cz (forthcoming).

[7] B Manolea et al "Qualitative study of UGC users and UGC non-users attitudes towards privacy, Work Package 8 of Consent" (2013) available at http://www.consent.law.muni.cz (forthcoming).

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 were particularly addressed. The survey was available online between July 2011 and December 2011. A total of 8,621 respondents from twenty-six 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 survey. Thus, the number of respondents to different questions varies 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 case 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 respondents was 30 years old. 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.[8] 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 authorised and committed and whether accepted user agreements are legally binding. Some users may consider these criteria as a hindrance, as users who do not meet one or more of these criteria may be excluded from UGC and SNS services. This is most apparent for age (C1.1). It is commonly accepted that SNS services are particularly something 'for the youngest generation'. According to research carried out within the EU Kids Online project, 59% of nine to sixteen year olds have a social networking profile.[9] From the perspective of minors, it is fair to state that social media are, in general, important to them. The Eurobarometer survey on "Attitudes on Data Protection and Electronic Identity"[10] found that "around 94% of the 15-24 year olds are using the Internet," compared to 66% of the EU overall 66%. 84% of fifteen to twenty-four year olds are using social networking sites (EU overall 52%) and 73% are using websites to share pictures, videos and movies (EU overall 44%). According to another recent study, 44% of teens have lied about how old they are online in order to

[8] 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 CONSENT website available at http://www.consent.law.muni.cz.

[9] S Livingstone et al "Risks and safety on the Internet: The perspective of European children" (2011) available at http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/D4FullFindings.pdf (accessed 12 Dec 13).

[10] Eurobarometer, "Attitudes on Data Protection and Electronic Identity in the European Union" (2011) available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (accessed 12 Dec 13).

access sites with age restrictions,[11] suggesting that such teens are younger than the required age for access. It should be noted that apart from obtaining access to particular websites, minors might have other reasons for lying about their age, such as their reputation among peers.

This is different for the capability (C1.2) and competence (C1.3) criteria to consent. According to the survey results, the majority of the respondents who read privacy statements indicated they completely understood (21%) the privacy statement or at least understood most parts (42%). It is important to note that these figures refer only to those respondents who indicated that they did in fact read privacy statements and thus does not apply to all respondents. However, the survey importantly revealed that most respondents never (27%), rarely (27%) or sometimes (23%) read the privacy statements.[12] Hence, most Internet users who responded to this survey question did not read privacy statements, whilst a comparably large portion of those who responded that they *do* read privacy policies show confidence in their understanding of such statements. Such results may be contrasted to the cited Eurobarometer survey, which found that 58% of European Internet users "usually" read privacy statements. Nevertheless, the fact that users feel capable of understanding (see also C4.1) the privacy statements does not imply that they do actually understand the privacy statements.

Most respondents (75%) sometimes, often or always watch for ways to control what they are sent online (such as tick boxes that allow opt-in or opt-out of certain offers). These results suggest 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 was confirmed by another survey question, which resulted in 82% of the respondents indicating that they "sometimes", "often" or "always" change their privacy settings when there are options available for personalising privacy settings.

In addition to low rates of privacy policy reading as mentioned above, most respondents (73%) indicated that they never, rarely or sometimes read the terms and conditions before accepting them. When users do not read the privacy statement nor the terms and conditions, they likely do not know what they have consented to. As a result, their consent is unlikely to be strong consent (C2.3) and up to date (C2.5). Whether 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 there is no research available on the link between not missing a particular website and the independence 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%) would be missed by users. Other websites are not missed (< 3%).

---

[11] Z Fox, "Nearly Half of Teen Internet Users Have Lied About Their Age" (2011) available at http://mashable.com/2011/12/13/teens-social-media (accessed 12 Dec 13).

[12] Importantly, this survey question included *all* Internet users, not merely UGC or SNS website users and thus included respondents who may only have an email account.

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 also routinely disclose personal data because of convenience, discounts, and other incentives, or a lack of understanding of the consequences.[13] As there may be long periods of time between a) data collection and b) actions based upon the processing or sharing of such information, the connection between such data collection and any resulting decisions may not always be transparent for individuals. For instance, when the personal data collected is used for profiling, such profiling techniques (by their nature) tend not to be visible to the individual.[14]

The fact that users are concerned about their privacy is also confirmed by the survey results, as to the question where respondents indicated on a seven point Likert scale (ranging from "not at all" to "very much") 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 preserve when online (mean 5.28, sd 1.59). Respondents clearly indicated which types of data they disclosed (C3.1) (which is largely in line with the Eurobarometer survey) and indicated their awareness of the purposes for which data controllers can and may collect, use and share personal data of users (C3.2). Most respondents (74%) indicated they were aware that their account or profile information may be used by the website owners for a number of purposes. Of these respondents, most were aware that this information can be used to customise the content a user sees (72%), to customise the advertising a user sees (79%) and to contact users by email (87%). There was also awareness, though less so, of other less publicised 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.

Regarding concerns for security measures (C3.3), the survey results indicated 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 above 50% and in some countries up to 90%. At the same time, the survey results suggested that most UGC and SNS users think it is unlikely that disclosing personal information on these websites puts their personal safety at risk. Similarly, respondents generally found it unlikely that they would become a victim of fraud, would be discriminated against or suffer reputational damage due to disclosures of personal information made online. These figures can suggest that many UGC and SNS users utilise their technical knowledge to protect themselves against physical or material risks and thus do not hold much concern in this respect. This contention is supported by the fact that users willingly disclose large amounts of personal information (see C3.1 above). However,

---

[13] P M Regan "Privacy and commercial use of personal data: policy developments in the US"(Rathenau Institute Privacy Conference, Amsterdam, Jan 2002).

[14] L A Bygrave *Data protection law; approaching its rationale, logic and limits* (The Hague: Kluwer Law International, 2002); B H M, Custers, *The Power of Knowledge; Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology* (Tilburg: Wolf Legal Publishers, 2004).

users may overestimate the quality of their security measures. For instance, users often choose easy-to-remember passwords, which are just as easy to breach.[15] For teens easily breached passwords may be a bigger issue, as nearly one-third (30%) of teens have shared a password with a friend.[16]

With regard to accountability of data controllers (C3.4), users want to know the data controller's reputation in order to decide whether to trust them.[17] Trust in online companies is limited. According to the Eurobarometer survey, 70% of European citizens are concerned about how companies use their data, exhibited by higher levels of trust in public authorities versus private companies – the latter including online social networks and other Internet companies.[18]

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 acceptance. This indicates that users may not be well informed about their rights. This hypothesis is confirmed in other research, indicating that users are not always aware (enough) of their rights and obligations with respect to sharing (personal) data.[19] It should be noted that users might also access other sources to inform themselves about their rights, such as consumer protection websites or the media. However, it is questionable whether such general sources can fully substitute the reading of the specific terms and conditions of a particular website. The conclusion that users do not 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.[20] 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.[21] Another possible explanation is 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 indicated that 'not reading' (i.e. not reading privacy statements) 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 included the concept of privacy itself being underdeveloped (particularly in some Eastern European countries) and a perceived helplessness that was often masked as disinterest in online privacy issues.

---

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

[16] Z Fox, see note 11 above.

[17] D Solove *The Future of Reputation* (New Haven: Yale University Press, 2007).

[18] Eurobarometer, see note 10 above.

[19] B Van den Berg and S Van der Hof "What happens to my data? A novel approach to informing users of data processing practices" (2012) 17 *First Monday*.

[20] D Hallinan, M Friedewald, and P McCarthy "Citizens' Perceptions of Data Protection and Privacy" (2012) 28 *Computer Law and Security Review* 263-272.

[21] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed 12 Dec 13).

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 level of detail in the privacy statements (C4.1) was presented as a concern for most respondents. Many respondents (55%) indicated that they do not read the privacy statements because they are too long to read. The fact that respondents to this question considered the privacy statements too long and detailed is also found in other research, where it was indicated that users of social network sites do not want to spend a lot of time reading privacy statements, on average 1-5 minutes.[22] However, most websites we analysed provide privacy statements that are much longer, often taking half an hour to read, and sometimes even an hour.[23]

Respondents to found the information provided for their consent decisions (C4.2) as understandable. As mentioned above, 64% of respondents indicated that they understand the information completely or mostly. Only 5% of respondents indicated that they do not understand the information at all. Of the people who do not read privacy statements, a mere 9% indicated that they do not read privacy statements because they are too difficult to understand. In the Eurobarometer survey a quarter of those who read privacy statements said they do not fully understand them.[24] 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. Users may become too confident and falsely believe that they understand everything. A large number of interviewees in the qualitative interviews claimed that they found the language used in privacy policies difficult to understand, The interviewees that did read privacy policies indicated that they viewed the reading as part of a learning process that is indispensable to assuming responsibility for one's personal information and thus be able to take adequate protective measures. However, even those readers expressed 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 data controllers in order to decide whether to trust them and, therefore, reliable and accurate information is important to them. Importantly, trust in online companies is limited.[25]

With regard to accessibility of the information provided (C4.4), of the 26% of the respondents indicating that they never read the privacy statements, only 4% did not know where to find privacy policies on a website. Similar patterns can be observed with other information, such as changing privacy settings. Most respondents to indicated that they change privacy settings. Of the people who never changed their privacy settings (18% of the respondents), 10% indicated that they did not know that privacy settings existed whilst 11% indicated that they did not know they could change the privacy settings. Hence, most people know where to find this information.

---

[22] B Van den Berg and S Van der Hof, see note 19 above.

[23] B Custers et al, see note 2 above.

[24] Eurobarometer, see note 10 above, at 112.

[25] Eurobarometer, see note 10 above, at 137.

4. Legal Provisions

Our next step was to determine the existence of legal provisions for each of the consent criteria in Table 1, and depending on their existence, to qualify these legal provisions. This was done as to the existing and proposed legal framework of EU personal data protection. An overview of the results is presented in Table 2. The existing EU legal framework is constituted by the Data Protection Directive 95/46/EC.[26] For more background on the EU data protection directive, we refer to further literature.[27] The proposed legal framework was published in January 2012 by the European Commission.[28] For more background on the proposed EU data protection regulation, we refer to further literature.[29,30]

4.1 Legal Provisions in the Existing EU Framework

The criteria for consent that are incorporated in the current EU Data Protection Directive are discussed in Section 4.1.1. The criteria that are not incorporated are discussed in Section 4.1.2. Some of the criteria are not included in the Directive, but are incorporated in other legal sources, such as regulations, policies, civil codes or legal practices. Most important among these sources is the Article 29 Working Party (Hereinafter "WP29"). WP29 is an advisory body to the European Commission on data protection issues and consists of representatives from the data protection authorities of each EU Member State. Although technically not part of the EU legal framework for data protection, the WP29 "Opinion 15/2011 on the Definition of Consent" is particularly relevant as it has given substance to the explanation of the Data Protection Directive's provisions on consent.[31] Several of the criteria for consent set out in Table 1 are addressed by the WP29's Opinion 15/2011.

---

[26] Directive 95/46/EG of the European Parliament and the Council of 24th October 1995, [1995] OJ L281/31.

[27] Z Fox, see note 11 above.

[28] *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF (accessed 12 Dec 13).

[29] C Kuner "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law" (2012) *Privacy and Security Law Report*.

[30] G Hornung "A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012" (2012) 9 *SCRIPTed* 64-81.

[31] Article 29 Working Party, "Opinion 15/2011 on the definition of consent" available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (accessed 13 Dec 13). (Hereinafter, 'WP29')

4.1.1 Incorporated Criteria

Informed consent must be reasonably strong (C2.3). This is described in Article 7 of the Directive, where unambiguous consent is mentioned as a general ground for lawfulness of processing someone's personal data. Article 8, considers the processing of special categories of (sensitive) data that would otherwise be prohibited, whereby explicit consent is included as one possible condition to lawfully process such data. Explicit consent means that the person who is giving the consent is aware of the issues are and what the consequences of his or her consent are. According to the WP29, unambiguous consent means that the procedure to seek and give consent must leave no doubt as to the data subject's intention to provide consent. For instance, consent based on disinterest (e.g. lack of complaint) is not considered unambiguous consent. The burden of proof for having obtained consent rests with the data controller.

The consent must be an independent decision (C2.4). This means that the decision has to be independent of the controlling influences of others. This criterion can be found in Article 2(h) of the Data Protection Directive, which states that consent has to be freely given. According to the WP29, consent is only freely given when the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent.[32]

It must be clear which data are collected (C3.1). On social network sites, it may be obvious which data are collected from the data subject, but when data is collected indirectly, this may be less obvious. It is important that a data subject knows which data is collected, so he or she can decide: whether this information is sensitive, whether it is relevant to the purposes of the data controller, whether the information is correct and complete, etc . Article 10 of the Directive requires the data controller to provide the data subject with information, including information about the existence of the right of access and the right to rectify the data. This means that the data subject has access to the data collected about him. Where the data controller has not obtained the data from the data subject itself, Article 11(1)(c) obliges the data controller to provide the data subject with information about the categories of data concerned and also about the existence of the right of access and the right to rectify the data.

In order to assess the consequences of providing consent, it should be clear for which purposes personal data are collected (C3.2). Article 6(1)(b) of the Directive requires that personal data only be processed if the purposes are specified, explicit and legitimate. Article 10(b) obliges the data controller to provide the data subject with the purposes of the processing for which the data is intended. Where the data has not been obtained from the data subject, Article 11(b) requires the controller to provide the purposes of the processing.

Some individuals may want to know what security measures are taken to protect their personal data prior to giving consent (C3.3). Article 16 of the Directive states that, in principle, personal data may only be processed on instructions from the data controller. Article 17 compels Member States to provide that the controller implements appropriate technical and organisational measures to protect personal data. However, the Directive does not require that users are informed about any such security measures.

---

[32] *Ibid.*

For the individual providing consent, it may be important to know the identity of whom is collecting and processing his or her personal data (C3.4). This can enable him or her to check the trustworthiness of the data controller. Some data controllers may have a good reputation, whereas others may be less reliable according to a data subject. It is also important to know who should be contacted in cases of incorrect or incomplete data. Articles 10(a) and 11(1)(b) of the Directive require the data controller to reveal its identity and the identity of its representatives, if any.

It must be made clear for the data subject which rights can be exercised and how they can be exercised (C3.5). Article 12 of the Directive contains the right of access, while Article 14 provides for the data subject's right to object and Article 15 the right for every individual not to be subject to decisions which produce legal effects concerning or significantly affects him or her, and which is solely based on automated processing of data. Article 13 allows Member States to adopt legislative measures to restrict the scope of obligations and rights provided in the Directive to safeguard national or public security, defence, criminal investigation, important economic or financial interests of the Member State or the European Union, monitoring, inspection or regulatory functions or the protection of the rights and freedoms of others.

The information provided must be specific and sufficiently detailed (C4.1). This follows from Article 2(h), provides that consent is 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed', whilst Article 6(1)(b) states that the purposes for processing data must be specified, explicit and legitimate. This also suggests that the data must be reliable and accurate (C4.3). The Directive does not require that the information provided be understandable or accessible, however the WP29 provides this as an extra requirement in their opinion on consent. Consent cannot be informed when the data subject does not understand the information provided. If the data subject has difficulties with accessing the information, this may inhibit the individual's ability to take note of and read the information.

Furthermore, the information provided should be reliable and accurate (C4.3). Article 6(1)(b) of the Directive states that personal data can only be collected for certain reasons. The data controller has to inform the data subject about what data he will process, for what reasons and for what time. In Article 10 and Article 11 of the Directive, it is specified what information the controller has to supply to the data subject in order to legitimately process that person's data.

4.1.2 Non-Incorporated Criteria

The Data Protection Directive gives no indication as to what age an individual has to reach in order to be able to give consent (C1.1). The requirements for legally valid consent by minors can be found in each Member State's national legislation; since this has not been harmonised, these requirements vary throughout Europe. In some Member States, for instance in the Netherlands, both the minor and his representative are required to give consent in order for it to be legally binding, unless the child is already deemed to be able to make an informed decision. However, the age at which a child is mature enough to make an informed decision, and the procedures to determine this, vary between the Member States. According to WP29, it is important to take the position of children into account when reviewing the Data Protection Directive; because of the lack of harmonisation on the general age of children to give legally

binding consent, there is no recognition for the need of special protection of children in specific circumstances. Additionally, the lack of a defined age for children to give consent causes legal uncertainty, particularly in the light of the international scope of most SNSs and UGCs.

The Data Protection Directive contains no special provisions for consent concerning individuals who do not have full legal capacity (C1.2 and C1.3). Member States have national provisions for consent by legally incompetent persons, but WP29 finds that the Directive should have additional provisions concerning the protection of this vulnerable group. WP29 raises a number of issues, which should be considered when reviewing the Directive:[33]

- Some of the provisions should include under which circumstances both the individual's consent and the consent of his representative are required;
- A provision concerning under which circumstances consent can be given by just the caretaker, without the individual's consent;
- Provisions clarifying in which cases consent is excluded from lawfulness;
- Provisions introducing (mandatory) use of online age-verification.

Written consent (C2.1) is not required by the Directive. Article 2(h) of the Directive describes 'any indication of his wishes (…) signify' as a way of providing consent. 'Any' indication of a wish is sufficient under the Directive. The Directive intentionally did not limit consent to 'written consent' in order to create a wide scope. The term 'indication' should be read in combination with the term 'signify' in the provision; the indication should include a wish, by which the data subject signifies his agreement. This 'signification' can include any form of behaviour by which consent can be reasonably concluded. However, passive behaviour seems to reach the lower limit of this provision; although the notion of 'indication' is wide, it seems to imply some need for action and, therefore, explicitness. At this point, it is also relevant to point out the difference between the 'regular consent' of Article 2(h) and the 'unambiguous consent' of Article 7(a) as a legal basis for processing. The WP29 states in its opinion on consent that:

> (…) unambiguous consent does not fit well with procedures to obtain consent based on inaction or silence from individuals: a party's silence or inaction has inherent ambiguity (the data subject might have meant to consent or might merely have meant not to perform the action).[34]

If there is partial consent instead of full consent (C2.2), personal data can only be processed for the purpose that has been consented to. However, in practice, and particularly in the online context, full consent is asked and required: the only option is either to accept or reject the terms and conditions under which personal data will be processed. Note that there are no legal obligations to provide options for partial consent.

The consent of the data subject must be up to date (C2.5), as it must match the actual data processing. However, data processing activities may change and expand over time. While there is no explicit requirement in the current Data Protection Directive

---

[33] WP29, see note 31 above.

[34] WP29, see note 31 above.

mandating that consent is 'up to date', this requirement may be inferred from the principles of purpose specification and use limitation (i.e. the data collected may only be used for the purposes specified in advance) as set forth in Article 6(1)(b). If the data subject provides consent for a specific, well-defined purpose, any substantial deviation from this purpose will require a renewal or confirmation of the consent.

Finally, the information provided has to be understandable and accessible (C4.2 and C4.4). Consent must be based on information provided beforehand. The provided information has to be sufficient to enable a person to make an informed decision about the processing of his personal data. According to WP29, two requirements derive from the fact that consent must be based on information. First, the information must be supplied in a language the data subject can understand, so the individual knows what is consented to. Information that is too technical or complicated, does not meet the legal requirements of Article 6. Second, the provided information must be clear and recognisable, so it will not be overlooked. It does not suffice to supply information somewhere random or hidden.

4.2 Legal Provisions in the Proposed EU Framework

The criteria for consent that are provided for in the current Data Protection Directive are similarly provided for in the proposed Data Protection Regulation. The relevant articles can be found in Table 2. However the proposed Regulation offers some additional criteria. These criteria (C1.1, C4.2 and C4.4) are discussed in this subsection. Our analysis of the proposed Regulation begins with the new definition of and conditions for consent.

In the proposed Regulation, the use of consent for legitimising data processing would be significantly restricted. The definition of consent is tightened in Article 4(8), since it must always be explicit (i.e. opt-in). The Regulation removes the current distinction between 'consent', 'unambiguous consent' and 'explicit consent', instead opting for a single definition of consent in Article 4(8):

> (…) the data subject's consent means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

The conditions for consent are further set out in Article 7:

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

The single biggest change in this new constellation is that consent, by means of an indication of wishes, is no longer recognised as legitimate (versus Article 2(h) under the current Directive). This means that under the new Regulation it may be argued that consent will need to be reasonably strong by definition, as it requires a specific, informed and explicit indication of wishes. This may have considerable consequences for companies engaged in e-commerce and online activities, for instance, by requiring an increased use of pop-up boxes and other mechanisms on websites that indicate a user's consent. This may conflict with Recital 25, which provides that electronic consent should not be unnecessarily disruptive.

Under the proposed Regulation there are now specific provisions for parental consent when children are below the age of 13 (C1.1). Article 8(1) provides:

> (…) in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorized by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

The European Commission may further specify the way in which consent can be obtained through delegated acts (Article 8(3) and Recital 129). Furthermore, the conditions for obtaining consent set out in Article 8(1) may not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Another relevant change in the context of consent is the more explicit requirements for information to be given to the data subject (Article 11), especially that this information is both understandable and accessible. (C4.2 and C4.4). First of all, the data controller must have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. Furthermore, the data controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

Table 2: Legal provisions for the criteria for consent

	Legal obligation in the *existing* Data Protection Directive?	Legal obligation in the *proposed* Data Protection Regulation?
C1.1	No, but obligation in most civil codes	Yes (Article 8), to be further specified in delegated acts (recital 129).
C1.2	No, but obligation in most civil codes	Obligation in most civil codes
C1.3	No, but obligation in most civil codes	Obligation in most civil codes
C2.1	No	No
C2.2	Yes, where required (Article 6(1)(b))	Yes (Articles 5(b)and 6(1)(a))
C2.3	Yes (Articles 7- 8)	Yes (Article 4(8))
C2.4	Yes (Article (2)(h))	Yes (Article 4.(8))
C2.5	No	No (but consent must match current practices)
C3.1	Yes (Articles 10, 11 (1)(c))	Yes (Articles 5, 14)
C3.2	Yes (Articles (6)(1)(b), 10(b), 11(1)(b))	Yes (Articles 5, 14)
C3.3	Yes (Articles 16-17)	Yes (Article 30)
C3.4	Yes (Article 10(a), 11(1)(a))	Yes (Article 14)
C3.5	Yes (Articles 12-15)	Yes (Article 14)
C4.1	Yes (Articles 2(h), 6(1)(b))	Yes (Article 14)
C4.2	No, but WP29 opinion sets this requirement	Yes (Article 14)
C4.3	Yes (Article 6(1)(b))	Yes (Articles 5, 14)
C4.4	No, but WP29 opinion sets this requirement	Yes (Article 14)

5. Gap Analysis and Solutions to Address Disconnections

In this section, a gap analysis will be made between, on the one hand, the results of the previous section (which criteria are addressed in the current and in the proposed EU legal framework) and on the other hand, the user expectations regarding these criteria (see Section 3). This gap analysis will show which criteria are insufficiently addressed from a legal perspective. From this analysis, suggestions will be drawn for both practical changes and changes in the legal framework to address any disconnects resulting from the gap analysis.

The proposed Regulation does contain specific provisions for parental consent (C1.1) and sets the age threshold at thirteen years old. Parental consent is only required for children until the age of thirteen under the proposed Regulation.[35] It also states that the data controller should make reasonable efforts to obtain verifiable consent. Furthermore, the proposed Regulation emphasises the risk that children cannot fully comprehend the dangers related to data processing (Recital 53). As such, the proposed Regulation does harmonise the age for consent to some extent and recognises that minors between the ages of thirteen-eighteen years old are very active on social media and require special protection (recital 29 and 38). We agree with this point of view,

[35] G Hornung, see note 30 above, p. 75.

which was also considered important by users, but note that there are little or no provisions in the proposed Regulation to make this special protection more concrete. Apart from notes on parental consent in Article 8, the only provisions relating to this issue are Article 33 (providing special focus on personal data of children when performing data protection impact assessments), Article 38 (special focus on child protection when drafting codes of conduct) and Article 52 (special focus on children when supervisory authorities promote awareness). These provisions ask for special attention to be given to children, but none of them substantiates how this should be achieved.

Another remark to be made concerns the enforcement of the provision in Article 8 regarding consent of minors. Although it should be mentioned that the proposed Regulation creates the opportunity for the European Commission to adopt delegated acts and lay down further standards for obtaining verifiable consent (paragraph 3 and 4 of Article 8), practical issues may arise. For instance, how can social media actually verify the age of their users? A simple click on a button stating "I am over eighteen" or "I am between the ages of thirteen and eighteen, but my parents consent to […]" may easily be abused, as minors may not tell their real age. According to a recent study, 44% of teens have lied about how old they are online to access sites with age restrictions.[36]

From other contexts, the practice of showing identification cards such as passports verifies age for purchase of alcohol and tobacco; however such age restrictions are difficult to apply in online situations. An online version of this practice may require introduction of an online age certificate, but that would involve a considerable (and costly) architecture. Moreover, an age verification scheme may raise new privacy issues, as it may entail more processing and sharing of personal data. Furthermore, it may limit the possibilities for anonymous use of SNSs and UGCs, or the use of pseudonyms. The available procedures to establish the authenticity of the parental consent (e.g. sending an e-mail from a parents e-mail account provided at the time of signing in, the provision of the parents' credit card details, a written consent form from the parent, or a telephone call from the parent) have been criticised for being easy to circumvent and workable alternatives have not yet emerged.[37]

Similarly, most UGCs and SNSs do not address the issue of whether a person is competent and authorised to use its services (C1.2 and C1.3). Some pose conditions, such as a minimum age threshold, whereas others, like Wikipedia, explicitly consider everyone competent. It may be suggested that people with limited capacities to navigate and use the Internet, for instance, due to psychological disorders or limited mental abilities, may deserve special protection – similar to those afforded to children. Neither the current Directive nor proposed Regulation offer such special protection. However, it should be noted that increased attention to different capacities and authorisation is not considered important by users. Furthermore, enforcement of requirements regarding competences and capabilities may be difficult, as UGCs and SNSs may include such requirements in their privacy statements but could experience difficulties in checking whether users actually meet these criteria. We recommend that the proposed Regulation is amended in such a way that this category of user is offered

---

[36] Z Fox, see note 11 above.

[37] E Bartoli "Children's Data Protection vs. Marketing Companies" (2009) 23 *International Review of Law, Computers & Technology* 35-45.

similar protection to minors, although we immediately note that this may raise the same issues as with minors discussed above: the proposed Regulation is not clear about how special protection is to be provided or on how enforcement will take place.

Written consent (C2.1) is not a legal requirement for consent, either in the current Data Protection Directive or the proposed Regulation. Although this is important to users, we think the main reason for not requiring written consent is because providing consent should be technology independent. With the rise of all kinds of multimedia applications, other forms of providing consent may become more common in the future. In such a situation, the requirement of written consent may turn out to be a hindrance. Nevertheless, written consent serves two main purposes: it removes the ambiguity from the consent, and it serves an evidentiary purpose. As such, in our view, written consent remains the preferred option.

With regard to partial consent (C2.2), most UGCs and SNSs offer possibilities to tweak privacy settings. Facebook even patented a method for profiling privacy setting selections of its users.[38] Users do appreciate and use such possibilities to personalise their privacy settings, including options for audience segregation. Hence, we recommend that such privacy settings offer more options and that they are brought to the attention of users more often. For instance, it may be suggested that privacy settings are part of the set-up or registration process. We also recommend more options for audience segregation, which is slightly different from the regular privacy settings. Most privacy settings are limited to setting the extent to which information is shared, whereas audience segregation involves showing different information from one particular profile to different groups.

It may be questioned whether the consent users provide to SNSs or UGCs is strong consent (C2.3). As indicated above, the CONSENT survey results provide indications that many users do not read the privacy statements and terms and conditions. Since we assume that consent should always be informed consent, we think reading and understanding the information provided, such as the privacy statements along with terms and conditions is important for establishing informed consent. However, users do not seem to think this is important. When looking at the practical methods in which users provide consent, this is often by ticking a box which indicates they have read (and sometimes that they have understood) the terms and conditions (and sometimes also the privacy statement). Although we recommend the use of tick boxes for reasons of clarity, unambiguity and explicitness, we think the use of tick boxes can be improved by only using tick boxes in which the terms and conditions are actually shown, as additional clicks may discourage users from further reading.

Whether 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. Some people have worries regarding the monopoly of some sites, such as Facebook,[39] whereas others

---

[38] N McAllister "Facebook's Zuckerberg awarded privacy patent" (2012) available at http://www.theregister.co.uk/2012/07/24/zuckerberg_privacy_patent (13 Dec 13).

[39] D Gillmore "Facebook's new business plan: from utility to monopoly" (2012) available at http://www.theguardian.com/commentisfree/2012/oct/08/facebook-business-plan-utility-monopoly (accessed 13 Dec 13)

think this is not a real concern.[40] Regular EU competition laws apply to these issues, but we will not discuss this in detail as we consider this beyond the scope of this paper.

Although users indicated in the interviews that they considered it important to be frequently updated on policy changes (C2.5), during our analysis of privacy statements we were surprised how outdated many of the privacy statements were.[41] More importantly, is that (according to the terms and conditions of most UGCs and SNSs) users often do not have to be notified about changes in the privacy statement. Most data controllers simply state that users have to check the website for any changes in the privacy policy. This is something that users obviously do not do. Therefore, we think a more active notification on changes is preferable. Furthermore, nearly all changes in privacy statements come from data controllers. Data subjects have no influence on the privacy statements. Of the websites analysed, only Facebook offered its users to influence policy changes, although the conditions set forth may be hard to meet. Instead of the current unilateral changes in privacy statements, changes based on shared ideas/beliefs of users may be preferable. Finally, we think updates on consent can be strongly enhanced by including sunset provisions in the consent decision. This means that consent should legally expire when it is not updated after some time, say within two or three years. This may ensure a more active notification policy of data controllers and prevents outdated consent.

Clarity regarding which data are collected, used and shared (C3.1) and for which purposes (C3.2) are important to users and sufficiently supported by the legal framework. We recommend more transparency regarding the data collected, used and shared, as most data are provided during the registration process and users may forget after some time which data they provided. Although we think that purpose specification is gradually losing meaning for several reasons,[42] there is a strong focus on purpose specification in EU data protection legislation.

Regarding concerns for security measures (C3.3), the survey results show that the portion of respondents applying various security measures is on average clearly above 50% and in some countries up to 90%. At the same time, the survey results showed that most UGC/SNS users think it unlikely that by putting personal information on these websites their personal safety is put at risk, that they risk becoming a victim of fraud or discrimination, or that they would suffer reputational damage. The resulting figures allow for the conclusion that many individuals use their technical knowledge to specifically protect themselves against physical or material risks – and, thus, do not show too much concern in this respect. Users may, however, overestimate the quality of their security measures. This hypothesis is supported by the fact that users easily share lots of information (see C3.1 above).

---

[40] T Worstall "Google, Microsoft, Apple, Facebook: Please, Will the Regulators Stop Worrying About Monopolies" (2012) available at http://www.forbes.com/sites/timworstall/2012/09/29/google-microsoft-apple-facebook-please-will-the-regulators-stop-worrying-about-monopolies/ (accessed 13 Dec 13).

[41] B Custers et al, see note 2 above.

[42] B Custers et al *Discrimination and Privacy in the Information Society* (Heidelberg: Springer, 2013), at 346.

In the current and proposed EU data protection legislation, security measures are an obligation of the data controller. We think this is a rather one-sided approach. When users are careless with their data and with security measures, data controllers can do little about this. We think that security is a joint responsibility of both users and data controllers. That does not mean that a user is always fully to blame for incidents when he of she has taken no security measures, but it does mean that users are to some extent responsible. We recommend that this joint responsibility is also expressed in the proposed legislation, for instance, by limiting the accountability of data controllers in cases of security breaches when users can be proven to have been very careless with their passwords, data or other security measures.

The identity and accountability of the data controller should be clear according to both the current and the proposed EU data protection legislation (C3.4). Users think this is important. We did not see any examples in which there is no compliance with this requirement. Therefore, we have no recommendations regarding this criterion.

Even though most privacy statements clearly indicate user rights (C3.5), 72% of the respondents never, rarely or sometimes read the terms and conditions before accepting them, indicating that users may not be well informed about their rights. Although users may also have access to other sources (such as consumer protection websites) to inform themselves about their rights, it can be questioned whether such (more general) sources could fully substitute the (more specific) user rights in privacy statements. Note that not reading privacy statements does not necessarily indicate disinterest. Only 7.4% of the respondents not reading privacy statements indicated disinterest as the main reason for non-reading. Other reasons were perceived helplessness, a more general belief in law and order or the perception that privacy statements served the protection of website owners rather than its users. These findings are confirmed by other research, showing that users are not always aware (enough) of their rights and obligations with respect to sharing personal data.[43] User expectations remain at a much more general and much less legally detailed level.

However, we expect that users are interested in their rights when something has gone wrong. As such, we recommend that user rights are also presented at the complaints site of a SNS or UGC. In most EU member states, users must go to court to enforce their user rights. It may be argued that for issues arising out of use of SNSs and UGCs, that this is a very high threshold; for instance, because of the costs involved. Other options may be less prohibitive. For instance, an option may be that complaints can be made to a national Data Protection Authority, who can then investigate the complaint, mediate or provide a decision or ruling. However, neither the current nor the proposed EU data protection legislation provides individual users with a right to make complaints at their national Data Protection Authority. We do not recommend this as the best option, but we do recommend consideration of other ways to address data controllers that are not compliant with data protection legislation. Having said that, we are convinced that the proposed EU data protection legislation does provide stronger measures for enforcement than the current legal framework.

The proposed EU data protection legislation also mentions a new user right: the right to be forgotten. It is questionable whether this right would mean any additional

[43] B Van den Berg and S Van der Hof, see note 19 above.

protection vis-à-vis the already existing right to erasure under the current EU Data Protection Directive.

Regarding specific and sufficiently detailed information (C4.1), users explicitly indicate that they do not want to spend much time on reading privacy statements. However, at the same time, they want to be informed properly. As straightforward solutions to this problem we suggest that information is offered in several layers, that summaries are offered and other tools are used to support the decision-making process of the consumer (such as machine readable privacy policies and visualisation tools, other than labels or icons).

Regarding understandable information (C4.2), users indicate that they do understand the information provided in privacy statements: 63.6% of the respondents of the survey indicated that they understand the privacy statements completely or at least most part of them. However, for those users that do not completely understand the information provided or for those users who overestimate themselves in this respect, we think there is room for improvement regarding the understandability of the information. We think legal jargon should be avoided and that the text should not be too long. Users do not have much interest in visualisations, such as icons or labeling.[44] The proposed Regulation mandates data controllers to have transparent and easily accessible policies (Article 11), but we think this is difficult to enforce, as it is difficult to determine whether policies are transparent and easily accessible.

We do think, however, that the understandability of privacy statements can be improved by having them read by representative groups of users. We do not know which SNSs and UGCs use this approach, but considering the fact that most changes in privacy statements are unilateral decisions of data controllers, we expect this is not a common practice. Rather, we think that most privacy statements (and terms and conditions) are drafted by legal experts in legal departments of data controllers, without prior review by individual users.

Although we have not seen any examples of information that is unreliable or inaccurate (C4.3), and although we do not doubt that most companies (particularly online companies) will take good care to protect their reputation by providing reliable and accurate information, it may be good to check the information provided for accuracy and reliability. However, this may be difficult to do for individual users, as they may not have insight into the data processing and other operations of SNSs and UGCs. Therefore, we think this is a task for national Data Protection Authorities. They could investigate whether the information provided does in fact reflect the practices (particularly data processing practices) within a SNS or UGC. The competences for such investigations are present in both the current Directive and the proposed Regulation.

Regarding the accessibility of information (C4.4), we have not seen any examples of: privacy statements that had to be paid for; that were in languages other than those of the targeted user groups; or that were behind a non-functioning link. The privacy statements we investigated were in fact easy to find. In most cases, there was a link to the privacy statement on every website of the SNS or UGC. Therefore, we do not think accessibility of the information is a major issue. SNSs and UGCs know they have to provide information and there do not seem to be any intentions to hide such

---

[44] *Ibid.*

information. The proposed legislation makes this even more explicit (Article 14). Therefore, we have no recommendations regarding this criterion.

6. The Limits of Consent

Before offering the conclusions of this paper, we would like to make a critical note. All recommendations made in the previous section are aimed at improving the current models for personal data protection and procedures for consent. However, in addition to improving the current models, we think it is also important to discuss the model itself.

The current models for personal data protection use the concept of informational self-determination as a basis. This concept can be traced to the work of Alan Westin,[45] who referred to privacy in terms of control over information, describing it as a person's right to determine for himself when, how, and to what extent information about him is communicated to others.[46] This indicates how, with the rise of information and communication technologies, the focus of privacy legislation has shifted from the protection of such things as family, home, and reputation towards the protection of personal information and informational self-determination.

Personal data protection was shaped in the 1970s and the 1980s as a set of principles on how personal data can be collected and processed in fair ways. In the US, this was done in the Fair Information Practice Principles (FIPPs)[47] and in Europe, this was done in the principles for fair information processing developed by the OECD.[48] The latter were later incorporated in the Treaty of Strasbourg[49] of the Council of Europe and in the current EU Data Protection Directive. All these principles boil down to a set of conditions under which personal data can be collected and processed (limited collection, data quality, specified purposes and limited use) and duties of data controllers (security safeguards, transparency, user rights and accountability).

When privacy is narrowed down to a set of principles for personal data protection, this has serious consequences for consent. In short, under the current Directive, consent legitimises nearly any form of collecting and processing personal data. At the same time, the current tools for informational self-determination do not provide data subjects significant ways to control the use of their personal data. For instance, in many situations, a user does not have any rights to have data deleted.[50] Furthermore, consent is often a take-it-or-leave-it situation: when a user does not consent to all

---

[45] A Westin, see note 5 above.

[46] For similar concepts, see C Fried "Privacy" (1968) 77 *Yale Law Journal* 475-493 and J Rachels "Why privacy is important" 323 *Philosophy and public affairs*.323-333.

[47] R Gellman "Fair Information Practices: A Basic History" (2012) available at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf (accessed 13 Dec 13).

[48] Available at http://www.oecd.org/internet/interneteconomy/oecd guidelines on the protection of privacy and transborder flows of personal data.htm (accessed 13 Dec 13).

[49] *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981* available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (accessed 13 Dec 13).

[50] The current Data Protection Directive mentions a right to rectify data, but not to have data erased when this data is correct.

terms and conditions of an SNS or UGC, in many cases he or she is plainly denied access.

Solove argues that the current models based on informational self-determination fail to offer adequate privacy protection.[51] He mentions several cognitive problems (on how people make decisions) and several structural problems (on how privacy decisions are architected), and why people are not even close to the model of informational self-determination. Basically, he argues, the model has too many hurdles: (1) people do not read privacy policies; (2) if they do read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed decision; (4) if people read them, understand them and can make an informed decision, they are not always offered the choice that reflects their preferences.

We think, together with Solove, that the current and proposed legislation, based on the model of informational self-determination, has many virtues and should not be abandoned. That is why, in this research, we tried to further improve the current models. But at the same time we notice that current models do not always reflect how people use SNSs and UGCs in practice. For instance, if a website has taken all privacy principles into account (which is normally the case), it means they have a sound and complete privacy policy (from a legal perspective), but 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. The survey results show that many people are unhappy with how their personal data is collected and processed, the choices they are offered and how their privacy is taken care of.[52] Hence, apart from optimising the current models, we think a further discussion on other, additional models is useful. Therefore, we strongly recommend further research in this area.

7. Conclusions

Based on our analysis, we conclude that both the current and the proposed legal framework address many, but certainly not all the aspects of consent that we investigated. The current Directive and proposed Regulation only provide a very general scope regarding consent and do not contain many details on how adequate consent procedures should look like. From our gap analysis it follows that there is, at some points, a disconnect between the abstract legal provisions and the concrete practical implementations in the architecture and privacy statements of SNSs and UGCs. These disconnects can be solved either by including more concrete provisions regarding the consent procedures in the legal framework or by changes at the practical level, such as architectural changes or changes in privacy statements.

Finally, we note that improving the current models for personal data protection, based on informational self-determination, and the procedures for consent derived from these models may not be sufficient to protect the privacy of social media users and meet their expectations regarding privacy and consent. Although optimising the current models in the proposed EU legislation has many virtues and the concept of informational self-determination should not be abandoned, further research is needed on additional models better reflecting how people use social media in practice.

---

[51] D Solove "Privacy Self-Management and the Consent Paradox" (2013) 126 *Harvard Law Review* 1880-1903.

[52] N Brockdorff et al, see note 6 above.