IDIS (2009) 2:65–79
DOI 10.1007/s12394-009-0017-3

Social networks and web 2.0: are users also bound by data protection regulations?

Brendan Van Alsenoy · Joris Ballet · Aleksandra Kuczerawy · Jos Dumortier

Received: 17 November 2008 / Accepted: 19 June 2009 / Published online: 1 October 2009

Abstract Directive 95/46/EC and implementing legislation define the respective obligations and liabilities of the different actors that may be involved in a personal data processing operation. There are certain exceptions to the scope of these regulations, among which processing which is carried out by natural persons in the course of activities that may be considered 'purely personal'. The purpose of this article is to investigate the liability of users of social network sites under data protection and to assess the extent to which the current data protection framework can sufficiently accommodate the new realities of web 2.0 and social networking applications.

Keywords Online social networks · Web 2.0 · User-generated content · Liability · Data protection · Scope · Personal use

Abbreviations

DPD	Data protection directive
ECHR	European convention of human rights
ECJ	European court of justice
SNS	Social network site(s)

Introduction

Online social networks are playing an increasingly important role in people's social, professional and cultural lives. The rapid growth in recent years, of the amount of

B. Van Alsenoy (✉) · J. Ballet · A. Kuczerawy · J. Dumortier
K.U.Leuven - Interdisciplinary Centre for Law & ICT - IBBT, Leuven, Belgium
e-mail: Brendan.Vanalsenoy@law.kuleuven.be
URL: www.icri.be
URL: www.ibbt.be

J. Ballet
e-mail: Joris.Ballet@law.kuleuven.be

A. Kuczerawy
e-mail: Aleksandra.Kuczerawy@law.kuleuven.be

J. Dumortier
e-mail: jos.dumortier@law.kuleuven.be

both social network sites (SNS) (Facebook, LinkedIn, Netlog, MySpace, ...) and their users, shows how important these new fora for social interaction have become. SNS provide participants with a means to transmit and share data with the people they know (and don't know) in ways that surpass traditional methods of communication. Due to their continuously growing technical capabilities and infrastructural setting (as internet applications), SNS offer individuals the opportunity to share information and develop vast social networks with greater ease and speed than previously possible. Another characteristic of most SNS is that they enable users to expand their circle of 'friends' to individuals they have never met in real life, and to interact with them in a wide variety of ways (instant messaging, picture sharing, games, group membership, …).

However, the new online social networks not only provide new opportunities, they also entail additional privacy risks. One could argue that these risks aren't as new as the opportunities themselves, but that the massive scale on which SNS deploy their services simply multiplies the chances of the risks being effectively manifested. A breach of confidence among friends is not uncommon in social relations outside SNS. However, the risk and potential damage of such a breach is significantly higher when, for example in the context of SNS, the threshold for 'friendship' may be lower and a large number of individuals are given access to personal data without discrimination.

The privacy risks that linger on the dark side of SNS, feed themselves by the (personal) data that are being processed through the services SNS provide. Certain studies indicate that users of SNS are aware of privacy risks, but are not always very concerned with the potential consequences (Goldie 2006: 150–153). The few mechanisms which are employed by the users of SNS to protect their privacy are generally limited to restriction of content (e.g. political opinions), relying on the anonymity (or pseudonymity) in SNS where available, or limiting the personal identifiable information they reveal (Goldie 2006: 154–157). Every individual is of course free to determine which aspects of his personal life he or she wishes to disclose. But what happens when SNS users include information relating to others in their social networking activities? The purpose of this paper is to analyze which actors (and to what extent) are responsible for compliance with data protection principles, under the framework set forth by Directive 95/46/EC (hereafter: "the Directive" or "DPD"). In particular, we seek to investigate the possible responsibilities and corresponding liabilities of users of SNS under the existing framework.

The Directive and implementing legislation define the respective obligations and liabilities of the different actors that may be involved in a personal data processing operation. Directive 95/46 also provides for certain exceptions to its scope, among which processing which is carried out by natural persons in the course of activities that may be considered 'purely personal'. Given the fact that most SNS are designed to house virtual circles of friends and personal profiles of its users (and are therefore primarily intended for recreational use), we must also examine the extent to which processing operations or entities may be exempted from complying with data protection regulations. The purpose of this analysis is to assess the extent to which the current framework can sufficiently accommodate the new realities of web 2.0 and social networking applications.

Misuse of SNS

SNS come in all sizes and shapes. However, their common 'raison d'être' can be found in the interaction between virtual identities of real life people. Most SNS require a profile from the user and foresee the possibility of establishing a network of relations. The interactions among virtual identities on SNS imply a continuous exchange of data, whether it be unilateral, bilateral or multilateral.

As indicated earlier, most SNS thrive on the willingness of users to exchange personal data and thus on their willingness to give up a part of their own privacy. Of course, social interaction, especially when dealing with members of your personal inner circle (e.g. family members, friends), ordinarily requires some release of personal information. The nature of the data being exchanged varies largely depending on the target-audience of SNS. LinkedIn for instance, is focused on education and employment, while other sites are intended to share sensitive data like health data.[1]

Privacy implications and risks typically associated with the potential misuse of personal data exchanged on SNS range from exposure to direct marketing, re-identification, profiling, identity theft, online and physical stalking, blackmailing and embarrassment. (See Gross and Acquisti 2005: 78–79)

Contemporary developments in case law have confirmed that privacy may also be jeopardized by 'ordinary' SNS users. A case recently decided by the High Court of England involved defamatory statements that were made by using a Facebook profile. (Applause Store 2008) The defendant had created a profile using the name of the plaintiff (MF) and created the group 'Has MF lied to you?', which was linked to the profile by hyperlink. The false profile contained defamatory content relating to the plaintiff and his company; and also revealed information as to the defendant's sexual orientation, his relationship status, his birthday, and his political and religious views. (Applause Store 2008: 3–4) The High Court found that these activities gave rise to a cause of action both for defamation and misuse of private information. No claims appeared to have been brought under the UK Data Protection Act however.

Countless scenarios can be imagined in which processing activities performed by a social network user would arguably constitute a violation of data protection principles. What if for instance a person was to create a public profile at a health-related SNS, in someone else's name, proclaiming that he suffered from a sexually transmitted disease? Or merely made a statement to that extent about another person on his own profile page? Or posted 'compromising' pictures involving other people than just himself?

In many instances, such conduct will be actionable on the basis of other grounds than the provisions of a Member States' data protection act (e.g. defamation, right of personal portrayal). However, not all claims give rise to the same extent of damages and may be subject to different exceptions. For instance, in many Member States, one of the lines of defense against defamation charges lies in proving the veracity of the stated facts. When there is no pre-existing relationship of confidence between the plaintiff and the defendant, a claim for misuse of private information under UK law

[1] See e.g. www.patientslikeme.com.

requires that the defendant acquired the information by 'unlawful or surreptitious means'. (See Brimsted 2008: 466)

It is in light of such possible restrictions that we seek to analyze to what extent the processing activities performed by SNS participants are subject to data protection regulations. Unfortunately, as we will see over the following sections, this issue is not entirely free of legal uncertainty.

Role definition

Actors

Under the framework of Directive 95/46/EC, there are at least two actors implicated for every processing of personal data: a controller and a data subject. A data subject is any individual to whom the information relates, provided that he or she is identified or sufficiently identifiable (art. 2, a). The controller is the entity who alone, or jointly with others, *determines the purposes and means* of the processing. It is also possible that the controller chooses not to perform all the desired processing operations entirely by himself, but to have a whole or a part of the processing operations carried out by a different entity. A 'processor' is then an entity who carries out such operations on behalf of the data controller (art. 2, e).

Directive 95/46/EC assigns practically all responsibility for compliance with data protection regulations to the controller. In the event the controller chooses to rely upon a processor for a whole or a part of the processing, he must bind the latter to only act in accordance with his instructions by way of a contract (see art. 17, par. 3). He remains liable however towards third parties.[2]

Given the fundamental importance of the qualification as either a controller or a processor, it is crucial to be able to determine in which capacity an entity is performing a particular processing operation. Despite this reality, technological developments since the enactment of the Directive have made it increasingly difficult to apply the distinction between 'data controller' and 'data processor' in practice. (Kuner 2007: 71–72) In order to illustrate this properly, we must depart briefly from the context of social networks.

Problems of qualification

At the time the Directive was adopted, the distinction was far clearer between parties who control the processing of personal data (data controllers) and those who only process the data on behalf of another entity (processors). (Kuner 2007: 71) Current business models for data processing are structured quite differently, and more and more parties divide their respective responsibilities in a way which does not allow for a clear distinction between data controller and processor. (Kuner 2007: 72)

[2] In the event that the processor violates his obligations towards the controller by exceeding his instructions, the controller will generally be able to take recourse upon the processor for the damages he incurred. However, the controller will in first instance have to defend the claims brought against him.

This is particularly the case when several autonomous (or relatively autonomous) entities collaborate to realize a certain application. The distinction especially becomes more clouded the more each participant has a stake in or receives some benefit from the processing. Much may be clarified by investigating the respective business models and practices of each entity involved, but it often remains debatable from what point an entity has sufficient input in determining the 'purposes and means' to be considered a controller. An additional factor which sometimes renders the distinctive roles less clear lies in the fact that the different collaborating entities may have been processing certain data for their own purposes prior to the collaboration.[3]

These developments have led us to adopt a less 'monolithic' conception of controllership with regards to personal data processing in which clearly distinct actors are participating. In the end, it becomes necessary to distinguish between the different types of processing operations and to determine which role each entity plays with regards to a particular processing operation. It is important to distinguish between the decision-making power concerning the overall structure of an application, its security features, its generic purpose etc. on the one hand, and the other hand the decision-making power that is exercised when deciding whether or not to make use of a particular application, which leads to the input of specific personal data. If both sets of decisions are made by the same entity, there is likely to be a single controller for that application. Otherwise there will most often be multiple controllers at work, though they are not necessarily to be qualified as 'co-controllers' or be jointly liable for the same processing operations. In other words, each participating entity might be considered a controller, but not necessarily for the same processing operations.

The approach we have outlined brings about two important consequences. First, it implies that for the same data exchange, which involves several separate actions, there can be more than one data controller, for the different actions that occur. Secondly, it hints that for a data exchange, the entity initiating the exchange may be considered to be acting as a controller with regards to its content. When an entity chooses to collaborate with others, and to share data it already had under its control for a different purpose, it bears the responsibility to assess the compatibility of the intended processing with the purpose for which the data was originally collected.[4] And if found not to be compatible, it shall in first instance be the provider of the data who will need to take the necessary measures to ensure that the intended processing shall comply with data protection (which may entail: obtaining a new informed consent, filing a new or expanding an existent notification, …).

The user of SNS as data controller

In order to be qualified as a controller, an entity must exercise at least some level of decision-making power with regards to both the purposes and means of a particular processing operation.

[3] This is increasingly common in the corporate world; where several relatively autonomous entities collaborate for instance to create a shared employee database. Other examples include the exchange of electronic health records among different hospitals, and the creation of interoperable eGovernment services involving different administrative entities.

[4] See art. 6, 1 b) DPD.

The purposes for which a user processes personal data within an SNS typically varies according to the type of SNS and the audience it seeks to address. In the majority of cases, users process data for purposes of social interaction or self-expression. Other purposes may include career development, self-education, … Every user can in fact freely determine the purposes of his processing within a given SNS.

As to determining the technical means of the processing, the user of an SNS generally does not have a great deal of decision-making power. While he may have the ability to adapt some minor features or settings according to his own wishes, he does not have any real power of negotiation as to the manner in which the processing is conducted. He either 'takes it or leaves it'. But every user does, as a rule, exercise the choice as to whether or not he wishes to provide a particular piece of information and of which application he makes use to do so. In this sense he still effectively determines the means of the processing when he entrusts data to an SNS.

This leads to the finding that users of SNS or web 2.0 applications may, at least in theory, be acting as data controllers. One must however be careful not to exaggerate the decision-making power of the individual user. The controllership of the user does not extend to the SNS as a whole, but only to those processing operations for which he can actually determine the purposes and means. The user of an SNS therefore only acts as a controller with regards to the *content he chooses to provide and the processing operations he initiates*.

It is important to note that the choices of the user are of course premised on his understanding of the functioning of the SNS. The role of the terms of use of the service will be discussed infra; under "Terms of use". In "Personal use" we will investigate to what extent the activities of an SNS user may be exempted from compliance with the Directive under the exception for personal use.

Liability of the SNS

The SNS service provider, from its part, determines its own purposes for processing. In most cases it offers its service to individuals primarily for the purpose of monetary gain. In addition to the operations that are strictly necessary to provide the service, this often implies additional processing activities; such as those serving to facilitate or enable direct marketing.

The SNS service provider determines practically entirely the means to achieve its purposes: it configures and operates the service expected by users, chooses how to make information available to third parties for marketing purposes, determines how much advertising space it shall foresee, etc.

Briefly put, the service provider determines both the purposes and means for the SNS as a whole. With regards to the actual content that is being distributed over the SNS, the service provider often exercises relatively little control at the moment this information is being uploaded by a particular user.[5] Nevertheless, it also acts as a controller when providing the service and distributing this information. Once the

[5] The SNS may of course induce the provision of certain types of information; e.g. by marking certain fields as 'required'. But even where the terms of use stipulate that the provided information should be accurate, there is no real guarantee that this shall in fact be the case.

personal data has been made available to it, the SNS provider proceeds to perform operations upon personal data of which it has determined the 'purposes and the means' in advance. Therefore the SNS provider may be labeled co-controller (together with the relevant users) with regards to the content being distributed over the SNS.

Some might say that this line of reasoning imposes too heavy a burden upon the SNS provider, arguing that in order to be able to provide an open service, the SNS provider cannot preventively 'screen' each request to create a profile or constantly monitor its application for any possible data protection violations instantiated by users.

This issue of liability of SNS providers is adjacent to the current controversy regarding the liability of web 2.0 service providers under the e-Commerce Directive (Directive 2000/31/EC). A full investigation into this matter falls outside the scope of this publication, which focuses more on the potential obligations of users of SNS and web 2.0 applications under data protection regulations. Suffice it to say for the moment that the e-Commerce Directive exempts certain service providers of liability for the content they may be hosting or transmitting provided certain conditions are met; but that it is still heavily disputed the extent to which web 2.0 service providers may benefit from these exemptions. (See Montero 2008)

Recital 47 of the data protection directive provides a basis to suggest a limitation of liability for the providers of electronic communication services for the content they transmit; but its language is clearly too specific to support an analogy for the providers of SNS.[6]

Exemptions of liability may however also be found in national legislation implementing the Directive. The Belgian Data Protection Act for instance provides that the controller of the processing shall be exempted of liability 'if he can prove that the injurious fact can not be attributed to him'.[7] The standard to assess whether or not an action or situation is attributable to the controller is one of reasonableness. The SNS provider can thus escape liability under the Belgian Data Protection Act if he demonstrates having continuously undertaken all reasonable measures to prevent the data protection violation from taking place, and to limit their effects once they have been manifested.

Terms of use

The contractual relationship between a user and the SNS he has joined is determined largely by the terms of use (privacy policy included) to which the user must consent prior to receiving the service. These terms are as a rule drawn unilaterally up by the

[6] Recital (47) of the DPD provides: "Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, *the sole purpose of which is the transmission of such messages*, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service".

[7] Art. 15bis of the Law of 8 December 1992 concerning the protection of privacy in relation to the processing of personal data, Belgian State Gazette, 18 March 1993.

SNS provider and in most cases stipulate that they may be modified by the SNS provider at will.[8]

However, the contractual relation between user and SNS is subordinate to mandatory regulations, such as the Directive and the national data protection acts.

Consequently the SNS (and user) are not entirely free to determine the attribution of roles and liabilities as controller or processor. The terms of use may modify the liability scheme for purposes of their (internal) relationship towards one and other, but this does not affect the rights of third parties. Every entity acting as a controller remains subject to suit by injured parties for violation of the data protection regulations, notwithstanding possible recourse by that entity in accordance with their contractual relationship (or exemptions of liability established by law).

The terms of use play an important role in defining the extent to which the user and SNS act as co-controllers. After all, the user's 'choice of means' is premised on his understanding of the functioning of the SNS. He can only subscribe to those means of which he is aware or has been notified. Only insofar as the SNS processes the data in accordance with the terms of use, can it be sustained that user and SNS act as co-controllers. Once the SNS proceeds to process data beyond the scope of what has been agreed in the terms of use–without obtaining the (explicit or implicit) consent of the user–the SNS will be qualified as the sole controller of the processing and bear the corresponding liabilities alone.

Personal use

We concluded in the previous section that the user of a social network may in principle be acting as a controller with regards to the processing operations he himself initiates. The question still remains however as to whether his actions fall within the scope of the Directive. The second indent of art. 3.2 provides that the Directive shall not apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity'. To what extent do users participating in social networks benefit from this exemption?

Recital (12) provides some, albeit limited, further guidance as to the scope of this provision. It suggests excluding personal data processing that is carried out by a natural person 'in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses'.

The terms 'purely' and 'exclusively' indicate that the exception for personal use should be construed narrowly, but both phrasings still leave room for much speculation seeing as they do not provide a clear standard as to what may or may not constitute a 'personal activity'.

The European Court of Justice (ECJ) has in one instance addressed this issue, namely when it was requested to issue a preliminary ruling in the course of the *Lindqvist* case. (Lindqvist 2003) Mrs. Lindqvist, who worked as a catechist in a local parish, had set up a number of web pages to provide information to fellow parishioners preparing for their confirmation. These pages also included information

[8] The consent of the user to the changes in the terms of use is usually inferred from the fact that he continues to use the SNS after the (notification of) the modifications. (See Terms of Use 2008).

about several of her colleagues in the parish, who were referenced either by their full names or merely by their first names. In many cases telephone numbers were listed. The pages also described, 'in a mildly humorous manner' the jobs held by these colleagues and their hobbies. Other information was also mentioned, such as family circumstances; and of one colleague it was stated that she had injured her foot and was working half-time for medical reasons.

Mrs. Lindqvist had not obtained the consent of the individuals referenced on her web pages, nor informed them of the fact that she was mentioning personal information about them. She also hadn't notified the data protection authority. She was subsequently prosecuted for violation of the Swedish law on personal data.

As to the question of whether the activities of Mrs. Lindqvist were covered by the exception for personal use, the ECJ replied that the exception must '*be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*'. (Lindqvist 2003: 47)

The Court appears to have put forward two elements to determine whether the exception of personal use is applicable. In the first place the processing activity must be carried out 'in the course of private and family life'. Secondly, the exception shall not apply where the data is published on the internet and made accessible to an indefinite number of people.

This clarification provided by the ECJ is most valuable to our further analysis; yet does not fully settle the matter. It precludes those instances in which the data is made available to an 'indefinite' number of people, yet does not specify a limit or threshold. The question also remains as to how one determines whether an activity is being carried in the course of private or family life. (See also Wong and Savirimuthu 2008: 256)

As to the latter question, several approaches can be imagined. A first possible approach could be to look at the *content* of the data. There one would seek to verify whether the information being processed could reasonably be related to the 'private sphere'. Such an approach must immediately be discarded however: the applicability of the Directive is not decided by the nature or content of the information being processed. (Article 29 Working Party 2007: 6) Furthermore, such an interpretation would lead to a situation where potentially highly sensitive information could fall outside the scope of the directive, whereas its ambit covers even information which may at first sight appear not to be privacy-sensitive or 'harmless'. (Article 29 Working Party 2007: 6)

A second approach could consist in evaluating the *quality or capacity of the recipients*. Relevant questions under this approach would include: does it concern a close friend or family member? Is there a sufficiently 'personal' connection among the entities involved? This approach taken by itself has the disadvantage of not taking into account that individuals might have both a professional and a personal relationship with each other. It might also lead to undue scrutinization of the level of intimacy between the entities involved.

A third, more comprehensive approach, answers the question of personal use by looking at the *context* of the processing activity. This approach can be aligned both with the language of the Directive and with the interpretation proffered by the ECJ.

The exception in fact concerns processing activities carried out 'in the course of' a personal or private activity.

It is noteworthy in this regard that whereas art. 3.2 of the Directive exempts data processing in the context of 'purely personal or household' activities, the ECJ makes reference to activities which are carried out in the course of 'private or family life'. The latter phrasing is nowhere to be found in the text of the Directive. It is arguable that this choice of words was instead inspired by the language of art. 7 of the EU Charter and/or art. 8 of the European Convention of Human Rights.[9] If the allusion to the terminology of these instruments was intentional, it could have significant ramifications for the scope of the exception for personal use.

It has long been established that the protection of 'private life' under art. 8 ECHR is not restricted to that which has historically been dubbed 'the private sphere'. Instead, the European Court of Human Rights has underlined that it also protects a right to identity and personal development, and the right to establish and develop relationships with others. (See e.g. European Court of Human Rights, P.G. and European Court of Human Rights, J.H. v. United Kingdom 2001: 56, European Court of Human Rights, Niemietz v. Germany 1992: 29) (See also Bygrave 1998) Bona fide users of social networks in first instance participate for purposes of social interaction. In addition, SNS also serve as a means for users to express themselves and develop their own (digital) identity. (See Goldie 2006: 139–142 and 160–162) Under this line of reasoning, it could be argued that bona fide participation in social networks should, at least in theory, be able to benefit from the exception for personal use. However, one may not lose track of the second element in the reasoning of the ECJ, namely that the exception shall not apply where the data is made accessible to an indefinite number of people.

The Belgian Privacy Commission, in a recommendation regarding the sharing of pictures by individuals (Belgian Privacy Commission, Recommendation 02/2007 2007), also touched upon the question of personal use. It considered that where images are processed for the sole purpose of distribution among a select ('definable') group of friends, family members or acquaintances, such processing could fall under the exception of personal use. As examples it mentioned the transmission of pictures via email to the participants of a family event, or the posting of such pictures on a secured website, which is only accessible to the relevant family members; and which is protected against indexing by search engines. (Belgian Privacy Commission 2007: 21–22) The Dutch Data Protection Authority adopted an almost identical approach shortly thereafter in its Guidance Report relating to the publication of personal data on the internet. (See College Bescherming Persoonsgegevens 2007: 12–13).

Users of SNS are often afforded the ability to choose whether their profile should be 'public' or 'private'. Private profiles are generally only fully accessible to other users marked as 'friends'. As regards to search engines, Facebook for instance appears to have opened up its application to indexing, but at the same time has given its users the opportunity to hide their profile from search results. But should these privacy settings of a user's account be a determinative criterion in assessing

[9] Art. 8 ECHR reads: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' (Council of Europe 1950) Art. 7 of the EU Charter reads: 'Everyone has the right to respect for his or her private and family life, home and communications.' (EU Charter 2000).

applicability of data protection legislation? The exception of personal use has been held not to apply when the data is made accessible to an indefinite number of people. Given the relatively low threshold many users set for deciding whether to accept someone as a friend (See Gross and Acquisti 2005: 73 and Boyd 2004: 1280. Contra: Goettke and Christiana 2007), should such weight in fact be accorded to users' settings? We would argue that the mere 'public' or 'private' setting of a profile by itself is too arbitrary a criterion, especially when considering the potentially great number of recipients even when the user has set his profile to private. In each instance it would still need to be verified whether the actions of the user can be considered as having been carried out in the course of a purely 'personal' or 'private' activity.

Implications

In the current state of the legal framework many SNS users shall be unable to avail themselves of the exception of personal use. Merely displaying a 'list of friends' strictly speaking amounts to personal data processing when the individuals listed are reasonably identifiable. SNS users will therefore almost certainly fall within the scope of the DPD when their profile is set to 'public'. It is still debatable whether users with 'private' profiles may benefit from the exception for personal use. In those instances the result is most likely to be determined on a case-by-case basis.

Needless to say, this outcome affects both malicious as well as 'bona fide' users of SNS. Every data controller is under the obligation to ensure that his processing activities comply with data protection regulations. This entails, inter alia, that they must ensure[10]:

- the legitimacy of the processing[11];
- respect for the data quality principles such as fairness, proportionality, finality and accuracy[12];
- that the data subject has the ability to exercise his rights towards the processing (right of access, rectification, erasure or blocking)[13];
- the confidentiality and security of processing[14];
- where required, that notification to national supervisory authorities is performed.

As a general matter, SNS profiles containing personal data relating to others should fall within the scope of the Directive; especially when these profiles are accessible to the public at large. It implies that profile owners must obtain the unambiguous consent of the individuals involved prior to posting any information related to them. It also brings about the obligation to remove any information the data subject perceives as harmful or undesirable when he or she exercises the right to object to the processing.

[10] The list provided here is not exhaustive. For a more extensive overview of the obligations of data controllers see (Kuner 2007).
[11] Art. 7 et seq. DPD.
[12] Art. 6 DPD.
[13] Art. 12 DPD.
[14] Art. 16–17 DPD.

On the other hand, we must also note that there are several provisions in the Directive and national implementations which may require some reconsideration or additional clarification. For instance, how does one interpret the requirement of not keeping personal data 'in a form which permits identification' for longer than is necessary (art. 6, 1, e) in the context of online social networks? Is it possible to determine a reasonable time-span as to how long a user should be allowed to maintain a picture or remark relating to another person on his profile page? Or may the data simply persist up until the moment that the data subject exercises the right to object?

Every controller is also obliged to inform the data subject of at least his identity and the purposes of the processing.[15] Strictly speaking, this implies that every user falling under the scope of the Directive is required to inform all data subjects referenced in his profile of his 'real-world' identity. Such a requirement may impose a significant limitation on the pseudonymous use of SNS, whereas several Data Protection Commissioners have only recently advocated that SNS providers should enable and encourage the creation and use of pseudonymous profiles. (Resolution on Privacy Protection in Social Network Services 2008) Of course data subjects may also be informed of the identity of the controller through alternative channels. But it is highly questionable whether such notification will take place in practice when no pre-existing relationship exists among them. One could argue that an SNS user must be willing to give up his pseudonymity if he or she decides to process personal data relating to others. But what if the only personal data relating to others in the profile is the user's friend list? Does every (reasonably identifiable) individual accepted as a friend then later have a claim to learn the real-world identity of the profile owner, regardless of whether or not he or she suffered any harm?

Closely related to the previous issue is the question of how other data subject rights are to be accommodated by the SNS provider and SNS users respectively. For instance, it may be assumed that if a data subject exercises his right to object towards the profile owner, the latter is under an obligation to remove this information from his profile immediately. However, what happens when the privacy policy of the SNS allows the provider to retain the data for a longer period of time? In the event of a dispute, may the data subject hold both the SNS user and SNS provider liable when only the latter proceeds to keep the data under his control? The SNS user may not be 'in control' of this further processing, but he or she was nevertheless responsible for the initial release of the data (cf. supra). The Directive currently does not explicitly require co-controllers to specify in a contract how data subject rights shall be accommodated. SNS users will have only limited or no negotiating power to see adequate provisions included in the terms of use.

The obligation to ensure the 'confidentiality of security of processing' also takes on a new dimension in the context of SNS. This requirement entails that the controller must ensure inter alia that the personal data which is being processed is only disclosed on a 'need-to-know' basis. When the user's profile is set to public, there is no restriction with regards to the entities that may access the information. But even where the profile is set to private, most SNS do not yet provide users with

[15] Art. 10–11 DPD.

great deal of freedom in determining which elements of their profile shall be visible to which 'friends'.

Liability towards data subjects for violation of data protection principles is not the only consequence of the qualification as data controller. It also brings about several formal requirements such as the obligation to file a notification with the supervisory authority mentioned in art. 18 of the Directive. Certain Member States have introduced exceptions to the notification obligation in their national legislation which may benefit social network users. In France for instance, the Commission Nationale de l'Informatique et Libertés (CNIL) decided to dispense certain web sites created by individuals from the notification obligation, for both the collection and distribution personal data. This exemption only applies insofar as this processing takes place in the course of 'a strictly personal activity'. (Commission Nationale de l'Informatique et des Libertés 2005) At the same time the CNIL emphasized that this does not dispense these individuals from complying with any of the other provisions governing the processing of personal data. They remain obligated to obtain the individual's prior informed consent, and must remove the data immediately if the data subject chooses to exercise his right to object. (Commission Nationale de l'Informatique et des Libertés 2005)

The Dutch Data Protection Authority has announced that their Ministry of Justice is considering an exemption to the notification obligation for 'personal publications'. Two additional conditions are expected to apply: the processing shall only be exempted if (1) all personal data is removed as soon as the data subject objects to the processing of his personal data and (2) the web pages containing personal data are protected against indexing by search engines. (College Bescherming Persoonsgegevens 2007: 29)

In other Member States, e.g., in Belgium, there has not yet been any indication of the intent to provide exemptions to the notification obligation for personal websites, blogs or social network activities.

Conclusion and outlook

At the time the Directive was being prepared, the European Parliament and Council could not foresee the fast development of social network sites, their popularity and impact on the privacy of users and non-users around the world. At that time, when individuals initiated personal data processing outside of a purely personal or domestic setting, in most cases they did so under the authority of an employer who was responsible for ensuring compliance with data protection regulations. Now, with the emergence of web 2.0 applications, every individual has the ability to distribute personal information to a large audience with great ease, and without needing a high level of technical proficiency. Seeing as this creates a setting in which the interests of third parties may easily be damaged, it is necessary that a clear legal framework is in place which governs the activities of SNS users.

In the previous section we have very briefly listed a few of the implications (and complications) of applying data protection legislation in the context of SNS. Many of the core provisions of the data protection directive could substantially benefit third parties who feel they have been wronged by information posted on an SNS

profile. But for several provisions it also appears difficult or unrealistic to apply them to SNS users with great rigidity. Seeing as the advent of web 2.0 brought along new opportunities for individuals, which could not be anticipated when the Directive was enacted, it is desirable that these issues be further clarified. We hope that the Article 29 Working Party includes them in their analysis when they adopt their opinion on on-line social networks. (Article 29 Working Party 2008–2009)

In this regard notice should also be taken of the report of the International Working Group on Data Protection in Telecommunications regarding privacy in social networks, which stated in its 'guidance towards regulators' that regulators should rethink the '*current regulatory framework with respect to controllership of (specifically third party-) personal data published on social networking sites, with a view to possibly attributing more responsibility for personal data content on social networking sites to social network service providers*'. (International Working Group on Data Protection in Telecommunications 2008) Whether or not more responsibility needs to be attributed to SNS providers is also still open for debate.

In any event, it is our opinion that further clarification, guidance and perhaps some revision of the existing framework is needed to accommodate the new realities of web 2.0 and social networking applications.

Acknowledgements The research leading to these results has received funding from the European Community's Sixth Framework Programme (FP6/2002–2006) under grant agreement n° 507512 (FIDIS NoE) and from the Seventh Framework Programme (FP7/2007–2013) under grant agreement n° 216483 (PrimeLife).[16]

References

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf. Accessed 15 July 2007.

Article 29 Working Party, Work Programme 2008–2009 of the Article 29 Working Party, WP146, 18 February 2008. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm. Accessed 15 April 2009.

Belgian Privacy Commission, Recommendation 02/2007 of 28 November 2007 concerning the diffusion of photographic material. www.privacycommision.be.

Boyd D. Friendster and Publicly Articulated Social Networks, in Conference on Human Factors and Computing Systems (CHI 2004), Vienna, ACM, April 24–29, 2004. http://www.danah.org/papers/CHI2004Friendster.pdf. Accessed 10 April 2009.

Brimsted K. The JK rowling photo case–are privacy rights evolving for the online era? CLSR. 2008;24:465–8.

Bygrave L. Data protection pursuant to the right to privacy in human rights treaties. Int J Law Inf Technol. 1998;6:247–84.

College Bescherming Persoonsgegevens, CBP Richtsnoeren–Publicatie van persoonsgegevens op internet, December 2007. http://www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf?refer=true&theme=purple. Accessed 10 April 2009.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2005–284 du 11 novembre 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère

[16] The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

personnel mise en oeuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (dispense n°6), J.O n° 293, 17 December 2005. http://www.cnil.fr. Accessed 16 April 2009.

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, available at http://www.echr.coe.int.

Data Protection and Privacy Commissioners, Resolution on Privacy Protection in Social Network Services, 30th International Conference of Data Protection and Privacy Commissioners Strasbourg, 17 October 2008. http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/08-10-17_Strasbourg_social_network_EN.pdf. Accessed 10 April 2009.

Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Official Journal of the European Union, n° L 281, 23 November 1995. p. 31–50.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal of the European Union, n° L178, 17 July 2000. p. 1–16.

European Court of Human Rights, P.G. and J.H. v. United Kingdom, 25 September 2001, Application no. 44787/98, available at http://www.echr.coe.int.

European Court of Human Rights, Niemietz v. Germany, 16 December 1992, Application no. 13710/88, available at http://www.echr.coe.int.

European Court of Justice , C-101/01, Bodil Lindqvist, 6 November 2003, O.J. 10 January 2004, C 7/3–7/4, available at http://curia.europa.eu.

European Union, Charter of Fundamental Rights of the European Union, O.J. 18 December 2000, C 364/1–22, available at http://www.europarl.europa.eu/charter.

Goettke R, Christiana J. Privacy and Online Social Networking Websites, Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, May 14, 2007. http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf. Accessed 21 October 2008.

Goldie JL. Virtual Communities and the Social Dimension of Privacy, University of Ottowa Law & Technology Journal. 2006;3.1:133–67.

Gross R, Acquisti A. Information Revelation and Privacy in Online Social Networks, in Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES'05), Virginia; 2005. p. 71-80.

High Court of Justice, Applause Store Productions Limited and Matthew Firsht v. Grant Raphael, 24 July 2008, [2008] EWHC 1781 (QB). www.bailii.org. Accessed 25 October 2008.

International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services–"Rome Memorandum", adopted 3–4 March 2008, Rome. https://www.agpd.es/portalweb/canaldocumentacion/internacional/common/pdf/wp_social_network_services.pdf. Accessed 27 October 2008.

Kuner C. European data protection law–corporate compliance and regulation. 3rd ed. New York: Oxford University Press; 2007.

Montero E. Les responsabilités liées au web 2.0, Revue du Droit Technologies de l'Information, 2008;32:363–88.

Terms of Use 2008 (accessed 31 October 2008):Facebook (http://www.facebook.com/terms.php?ref=pf; http://www.facebook.com/policy.php?ref=pf); Myspace (http://www.myspace.com/index.cfm?fuseaction=misc.terms; http://www.myspace.com/index.cfm?fuseaction=misc.privacy) Netlog (http://nl.netlog.com/go/about/legal/view=general; http://nl.netlog.com/go/about/legal/view=privacy).

Wong R, Savirimuthu J. All or nothing: this is the question? The application of article 3(2) Data Protection Directive 95/46/EC to the internet, J. Marshall J. Computer & Info. L. 2008; 25:241–66.