transformation test and declare software patents invalid[55] while others asked that software patents be declared abstract and, therefore, not recognized patentable subject matter under section 101.[56]

The Supreme Court did not have enough votes to either affirm or disavow software patents. Justice Kennedy and three other Justices spoke out in favor of protecting software patents in the Kennedy plurality opinion. Justice Kennedy noted that "times change," and although established principles of patent law weighed against patentability of computer programs, "this fact does not mean that unforeseen innovations such as computer programs are always unpatentable."[57] Justice Kennedy noted that the machine-or-transformation test was adequate for the Industrial Age, but not for the Information Age. Justice Scalia and the four liberal justices did not address software patents.

Although the Supreme Court majority did not directly affirm software patents, it left the door open to patent protection for software that can be tied to a particular apparatus under the machine-or-transformation test, as well as software that is not abstract. Given that *Bilski* did not involve any software patent claims, it is possible that the Supreme Court is waiting to address this issue at greater length in a future case that is directly on point. Until then, the PTO guidelines issued by Commissioner Bahr are the only guidelines that are available. Again, there is also the possibility that Congress will address the issue of software patents in future patent reform to prevent the courts from having to guess at its intent.

IV. Conclusion

The *Bilski* decision is of great importance for several reasons. It reiterated the Supreme Court's position that a rule-oriented approach to patent law is not appropriate. The Court emphasized that the Federal Circuit's rigid use of the machine-or-transformation test was not supported by the text of section 101 of the Patent Act.

The decision furthermore revealed a split among the Justices over business method patents, and, to a lesser degree, software patents. Although some law firms have treated the case as soundly rejecting the call to outlaw business method and software patents,[58] this is not the case. The *Bilski* decision instead shows that the liberal justices support a strict reading of section 101 and that most of the conservative justices advocate interpreting section 101 to encompass technologies not contemplated by Congress at the time the Patent Act was passed.

Because of this division in the Court, businesses must keep a careful watch on developments in the PTO and Federal Circuit for guidance on which methods are patentable and which methods are too abstract to merit protection. Moreover, it would not be surprising if the Supreme Court granted certiorari on a future case that directly addressed the patentability of software. For now, companies would be best advised to carefully study the Court's precedents in *Dier, Flook*, and *Benson* to help understand what constitutes an abstract claim.

Software (Oct. 1, 2009), available online at *www.redhat.com/about/news/prarchive/2009/bilski.html* (last accessed July 15, 2010).

55 *Id.*

56 *See* Google Brief.

57 *Kennedy* slip op. at 8.

58 *See, e.g., Supreme Court's Bilski Decision Soundly Rejects Call to Outlaw Business Methods Patents*, Goodwin Procter Alert (Jun. 30, 2010), available online at *www.goodwinprocter.com/Publications/Newsletters/Client-Alert/2010/Supreme-Courts-Bilski-Decision-Soundly-Rejects-Call-to-Outlaw-Business-Methods-Patents.aspx* (last accessed July 15, 2010).

Natali Helberger/Joris van Hoboken

Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers

Much of the privacy problems on Social Network Sites (SNSs) are user-made. Yet, so far only few commentators have volunteered to discuss the legal consequences of all that privacy infringing behaviour. To what extent does the law place legal obligations on SNS users to respect data protection principles? Do amateur users qualify as 'data controllers' and can they as such be held fully liable for compliance with data protection law? One of the few that did address this question was the Article 29 Data Protection Working Party, an EU institution composed of the national data protection authorities. It concluded that, under certain circumstances, amateur users could indeed be considered data controllers. The Working Party was quick, however, to emphasize that these situations would be the exception rather than the rule. It also did not elaborate much further on the legal consequences for amateur users were the rules to apply to them.

This article will argue to the contrary that the instances in which amateur users will fall under the ambit of data protection law are not the exception, but rather the rule. It will then take the idea of the amateur data controller further, until the bitter end so to speak. Based on an analysis of the provisions of the European Data Protection Directive, the article will demonstrate that existing data protection law burdens amateur users with provisions that exceed the personal, technical and financial capacities of most SNS users, that do not fit the SNS context or that users are simply not able to comply with without assistance from the SNS provider. While it is unaccept-

▷ Dr. Natali Helberger/Joris van Hoboken, Amsterdam. Further information about the authors at p. 128. The authors would like to thank Prof. Dennis Hirsch, Prof. Ronald Leenes, Prof. Egbert Dommering, Sjoera Nas, Frederik Borgesius and Bart van der Sloot for their thoughtful and thought-provoking comments and suggestions. All omissions and mistakes are entirely those of the authors. The authors would also like to thank the Netherlands Organisation for Scientific Research (NWO) whose funding made the writing of this article possible. Parts of this article are based on findings from a study that the authors conducted for the European Commission on User Created Content (UCC) in 2008, infra note 36.

able to burden amateurs with a number of obligations that exceed their capacities, it is also not feasible to place all the burdens on SNS providers, since many of the privacy problems of SNSs are in fact user-made. All this points to a concept of joint-responsibility of SNS users and providers. The article concludes with a number of concrete suggestions on how such a concept of joint responsibility could be given form.

For the purpose of the analysis the terms of use and privacy policies of a number of the leading SNS sites in Europe were analysed, including MySpace, Facebook, Netlog, Bebo, Skyblog and Flickr.

I. Starting Points: EC Data Protection Law and The Concept of the 'Data Controller'

Authors who reflect about privacy and Social Network Sites like to speak of a "privacy paradox".[1] While experts deliberate on how to improve the protection of SNS users, the very same users continue to scribble, tag, kudo and share their personal data with the rest of the world. Much of the content that they upload is personal, including baby pictures, holiday videos, and evidence from last night's party. Users tend to share not only their own personal information very truthfully, but also the personal details about friends and family. As a GetSafeOnline survey revealed: 27 % of 18–24 year-olds UK SNS users admitted that they have posted information about and photos of other people without their consent online.[2] And, according to a Pew study, between 58 % (boys) and 72 % (girls) of teen users of SNSs publish photos of their friends.[3] There is no denying that a serious risk to the fair processing of personal data on SNSs are users and their friends. Little brother is tagging you. This section will explore if 'little brother's' activities make him a data controller in the sense of the law.

The European Data Protection Directive (hereinafter 'DP Directive')[4] regulates the 'processing' of 'personal data' by assigning a set of relatively open obligations to 'data controllers' and corresponding rights to 'data subjects'. The scope of the DP Directive is broad. Basically, any operation which can be performed upon information counts as 'processing'. Personal information is defined as any information relating to an identified or identifiable natural person, whereas an identifiable person is one who can be identified directly or indirectly.

Looking at SNSs, it is clear that a variety of personal data is being processed. This includes the users' registration data (collected by the service provider), their extended profile (typically including name, location, date of birth, profile picture, occupation, preferences, friends), their user data (registration of the users' activities on the service, not involving publication) and publications relating to themselves, other users or third persons (personal data in stories, pictures, videos, tags, etc.) The following section will concentrate on the last category, i.e. personal data posted by SNS users. For all this processing of personal data, the question is who is (or who are) the data controller(s)?

The Directive defines the data controller as the entity *"which alone or jointly with others determines the purposes and means of the processing of personal data"* (Article 2 DP Directive). Notably, the Article 29 Working Party adopted an opinion about the legal concept of controller.[5] Regarding the situation of social networks, the Working Party stipulates that *"[s]ocial network service providers ... are data controllers, since they determine both the purposes and the means of processing of such information. The users of such networks, uploading personal data also of third parties, would qualify as controllers provided that their activities are not subject to the so-called 'household exemption'"*. The Working Party mentions the case of social networks as an example for a situation of joint responsibility.[6] The Working Party further refers to its former opinion 5/2009 on social networking which specified that providers of social network services are to be considered data controllers because *"[t]hey provide the means for the processing of user data and provide all the 'basic' services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties."*[7]

As regards the possible data controllership of the end-user, the opinion on social networking proceeds in three steps. First, the opinion states that SNS users should typically be considered data subjects, seemingly in their relation with the service provider.[8] Second, it points to the household exemption as a quasi default rule for any "individual who processes personal data *"in the course of a purely personal or household activity"*. Third, it dis-

1 *S. Barnes*, 'A privacy paradox: social networking in the United States', First Monday, Vol. 11, No. 9–4 2006. *S. Utz* and *N. Krämer*, 'The privacy paradox on social network sites revisited: The role of individual characteristics and group norms', Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3(2), 2009 available at *www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2*. Explaining why user behaviour on SNSs is less paradoxical than it might seem in the first place: *R. Leenes*, "Context is Everything, Sociality and Privacy in Online Social Network Sites, to appear in *Simone Fischer-Hübner, Marit Hansen*, etc (eds), PrimeLife/IFIP Summerschool 2009; presented at the Hawaii International Conference on System Sciences, Kauia, Hawaii, 4–7 January 2006, IEEE Computer Society, available at: *www.danah.org/papers/HICSS2006.pdf*; *J.L. Goldie*, 'Virtual Communities and the Social Dimension of Privacy', 3 University of Ottawa Law & Technology Journal 1, 2006, p. 133–165. For a discussion of the role of social pressure, see e.g. Ofcom, 'Social Networking. A quantitative and qualitative research report into attitudes, behaviours and use', Research document, 2 April 2008, available at: *www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/*.

2 See e.g. Get Safe Online, 'Social Networkers and wireless networks users provide "rich pickings" for criminals', *Get Safe Online Week*, 12 November, 2007, available at: *www.getsafeonline.org/nqcontent.cfm?a_id=1469*. See also *S. Hinduja* and *J. Patchin*, 'Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace', 31 *Journal of Adolescence* 2008, p. 125–146.

3 Pew Internet, 'Teens, 'Privacy & Online Social Networks, How teens manage their online identities and personal information in the age of MySpace', report, 18 April 2007, p. 18, available on: *www.scribd.com/doc/2475365/Teens-Privacy-Social-Networks*.

4 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, OJ L 281, 23 November 1995, p. 31–50.

5 See Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010 (WP 169), p. 21.

6 *Ibid.* p. 21.

7 Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, adopted on 12 June 2009 (WP 163), p. 5.

8 Although correct as a general statement, the Working Party thereby confuses the definitions of 'data controller' and 'data subject'. In particular, the opinion does not address the possibility that the data subject is the only data controller as regards the processing of certain personal data, such as in the case of a natural person who publishes a collection of personal information relating to his/herself on his/her own website.

cusses a number of typical circumstances in which the household exemption would no longer apply, such as for publicly accessible profiles or the processing of personal data in the course of professional use of SNSs.[9]

II. SNS Users and the Household Exemption

Individual users would not have to comply with the provisions of the DP Directive if the Directive's household exception applied to their activities. The Directive provides little guidance on the scope of the household exemption. Article 3 (2) DP Directive 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."* Recital 12 of the Directive adds the characterizations *"exclusively personal or domestic"* and gives two examples of such processing, namely *"correspondence and the holding of records of addresses"*.

The European Court of Justice addressed the scope of the household exemption in its infamous Lindqvist judgment, in which it upheld a Swedish fine for Mrs Lindqvist's publication of information about fellow church volunteers on her personal website. The Court concluded that the household exemption *"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."*[10] In other words, if data are made accessible to an indefinite number of people, the household exemption does not apply.[11] This line of reasoning of the Court is consistent.[12]

An important and unanswered question about the scope of the household exemption is whether the factual circle of the processing of the personal data involved always has to be confined to the personal or household sphere. This question has become particularly pertinent with the rise of cloud computing, which has led to a situation in which hardly any processing of information is confined to the factual personal sphere. If the answer to this question is in the affirmative, the household exemption becomes almost meaningless.

The Article 29 Working Party, when discussing limitations on the scope of the household exemption, focuses on both the actual data processing and its purposes. In its opinion on the concept of personal data, it already mentioned the relevance of "the intention of use (for purely personal or household activities by a natural person)."[13] In its opinion on social networking it names two circumstances in which SNS users would not be covered. The first relates to the purpose and nature of the use of the SNS. *"If an SNS user acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the exception does not apply."*[14].

The second circumstance mentioned by the Article 29 Working Party relates to the accessibility of the personal data on the service and on the Web more generally. It considers a high amount of contacts an indication of the inapplicability of the exemption.[15] The Working Party did not clarify what constitutes a *"high number of third party contacts"*. It notes that if a user takes *"an informed decision to extend access beyond self-selected 'friends' data controller responsibilities come into force"* and the *"same legal regime"* that applies for professional data controllers will also apply to amateurs.[16] This again highlights the importance of availability and use of technical measures to restrict access (see also section 5).

The Working Party's discussion of the scope of the household exemption offers little practical guidance, except to the extent that it does not consider the possible obligations on SNS users as data controllers a priority. In reality, a substantial share of amateur users use SNSs not only (or not exclusively) for purely personal purposes, but also for professional networking, as well as political, commercial or charitable ends. In addition, profile information is often accessible to search engines and the Web more generally. The amount of 'friends' often extends to several hundred, some of which the person involved will not even remember. In other words, individual users acting as data controllers will be the rule rather than the exception.[17] Quite possibly, the Working Party was mostly interested in addressing the responsibilities of SNS providers.[18] Its discussion of the household exemption for SNS users serves the purpose of making a pragmatic distinction between these two categories of possible data controllers. By focusing in the first place on privacy issues related to SNS providers, the Article 29 Working Party failed to shed more light on the proper involvement and responsibility of end-users of SNSs. The users are in many cases the primary perpetrators of privacy infringements on social networking sites. Seeking to solve these privacy issues by suggesting obliga-

9 The Article 29 Working Party does not discuss the remaining responsibility of the SNS provider. It seems to be of the opinion that the provider is (or remains) a data controller in relation to the data processed by the user which is covered by the exemption.

10 ECJ, 6 November 2003, C-101/01, CR 2004, 286 – *Lindqvist*, para. 47.

11 Notably, the ECJ's Advocate General also addressed the household exemption in her opinion in the Promusicae case. The A-G seems to base her reasoning of the absence of a household exemption for data processing by electronic communications providers on the technical characteristics of these services: *"The bringing of civil proceedings against [...] Promusicae and the processing of connection data by Telefónica are not to be categorised as personal or household activities. That is also apparent, with regard to the processing of connection data, from the existence of Directive 2002/58, which does not include the exemption for personal and household activities, but assumes that the processing of personal data by providers of electronic communications services is in principle subject to data protection.[...]"*. See Opinion of Advocate General *Kokott* delivered in Case C-275/06, 18 July 2007 "Promusicae", para 58.

12 ECJ, 16 December 2008, C-73/07, "Satakunnan Markkinapörssi and Satamedia", para. 44: "It follows that the latter exception must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals (see Lindqvist, paragraph 47). That clearly does not apply to the activities of Markkinapörssi and Satamedia, the purpose of which is to make the data collected accessible to an unrestricted number of people."

13 See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP 136), p.4.

14 Article 29 Data Protection Working Party 2009, supra note 7, p. 6.

15 *Ibid*, p. 6.

16 It is possible that the SNS provider does not accommodate such a choice. Arguably, the user then still chooses to extend the accessibility of the profile, by his or her choice to use the service.

17 In this sense probably also *B. Van Alsenoy*, et al., 'Social networks and web 2.0: are users bound by data protection regulations?', Identity Journal 2009, Vol. 2, No. 1, p. 74–75, with reference to the legal situation in Belgium and the Netherlands.

18 The Article 29 Working Party was not the only regulator addressing SNS provider responsibility for privacy issues. See e.g. Office of the Privacy Commissioner of Canada, Report of findings into the complaint, filed by the CIPPIC against Facebook Inc., 16 July 2009. For a discussion, see *Beardwood* & *Stern*, 'Regulating Social Networking: Lessons from Canada', CRi 2009, 170–175.

tions for the services that make privacy infringing behaviours possible is like trying to prevent drunk driving by regulating car manufacturers.[19]

III. Users As Data Controllers

To conclude that individual SNS users do qualify as data controllers under the Directive means that they will have to comply with data protection obligations like any other (professional) data controller. European data protection law has neither been written with application to amateur users nor to social networks in mind. The following section will discuss some of the possible implications when applying existing data protection law to individual SNS users.

Arguably, some provisions in existing data protection law can be applied, at least in theory, very well to individual users, and the overall effect on the respect for privacy and fair processing of personal data on SNS could be positive. For example, it is well-conceivable that amateur users as a rule of thumb should be required to ask for their friends' consent before publishing their photos or personal information.[20] Respecting the privacy of their friends should be a self-evident element of any SNS netiquette, particularly but not only in case of profiles that are open to the public.[21] When asking their friends for consent, it is, arguably, only logical to provide friends with information about the publication of their personal information, including the purpose of the publication and who will have access to the data (e.g. whether a site is password protected and only accessible to friends, according to the requirements of Art. 10 of the Directive). It is, however, also necessary to understand that the behavior and expectations of users of SNSs will depend to a considerable extent on social norms and conventions within the respective community or circle of friends. Although a worthy subject for future research, it would go beyond the scope of this article to discuss the possible interaction between social and legal norms. Possibly, clarifying that SNS users can be held legally responsible could make users behave more responsibly when sharing information about others, and so ultimately also influence social norms and habits.

In practice the application of these provisions might raise a number of difficult questions: from the perspective of most users, notions such as "personal data", "sensitive data",[22] and "consent" are abstract terms with little practical meaning. Probably even more detached from the personal experience of amateur users is the fact that according to the law they would have to inform their friends before implementing certain widgets or applications that also access friends' data,[23] or the obligation to inform their friends about the existence of a right of access to and the right to rectify data (Article 12 of the DP Directive). Most amateur users will not be aware that they themselves possess such a right, not to speak of the fact that they could be obliged, by law, to grant this right to their friends. In other words, compliance with many provisions in data protection law probably exceeds the knowledge and experience of most users.

1. Consent and Data Accuracy

Next, there are a number of provisions that simply do not fit the SNS context and related social practices. Will friends, when asked for consent, actually be "able" to say no, or will social pressure prevent them from doing so? Also the reliance on passwords and technical protection measures can conflict with actual habits on SNSs. An Ofcom study found that by not revealing sensitive personal information, users can actually risk social exclusion. Particularly younger users indicated that [t]hey wonder, 'when the whole purpose is to find people and communicate, why anyone would hide personal details, and [that they] are suspicious of what such a person has to hide.'[24] Another example of a "bad fit" is the obligation in Art. 6 of the DP Directive to make sure that personal data of others is accurate and up to date, as well as to delete data that is inaccurate or incomplete. This provision is appropriate and understandable in the context of professional data collections. However, it can lead to bizarre results if applied in relation to individual users. Would it mean, for example, that if I had chatted about the new boyfriend of my friend Emily on my profile and they broke up, that I am obliged to correct my earlier entries and inform everyone that they are no longer an item?[25] Again, the situation is the result of the fact that the communication and exchange of personal profile information on SNSs is largely of a personal nature, as opposed to the purposes behind professional data processing, for which these rules were written in the first place.

2. Data Loss Prevention

There are a number of obligations under data protection law that individual users are simply not able to comply with, at least not without cooperation from the SNS provider. One example is Art. 17 DP Directive, according to which data controllers must implement the "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, disclosure or access" and against all other forms of unauthorized processing.

19 Compare *J. Grimmelmann*, 'Saving Facebook', 94 Iowa Law Review 1137, 2009. *Grimmelmann* gives the example of 'ghost riding the whip', which involves jumping out of a driving car and points out that policy makers interested in addressing the dangers of ghost riding would be better off focusing on the ghost riders than the car manufacturers. The key issue in the context of SNS, *Grimmelmann* argues, is to focus on the social dynamics of social networking technology use.

20 According to Art. 7 of the Data Protection Directive, personal data may only be processed if the data subject has unambiguously given her consent, unless one of the exceptions in Arts. 7 b)–f) apply (none of these exceptions seem to fit particularly well the situation of the amateur user, except for Art. 7 f.) of the Data Protection Directive, which can in particular be used to balance the expressive interests of a data sharing user with the privacy interests of data subject(s). In case of sensitive data, more stringent norms apply.

21 Differentiating Pew Internet 2007, p. 20, exploring what kinds of information teens themselves feel that should (not) be shared in public, supra note 3.

22 It's worth noting here that some courts, including the Dutch Supreme Court, have concluded that pictures of natural persons are sensitive data because they reveal their race. See Hoge Raad [Dutch Supreme Court] 23 March 2010 (Translink). Also the European Court of Human Rights has stressed the right of data subjects to in their image. See ECHR, 15 January 2009, *Reklos and Davourlis v. Greece*.

23 See e.g. *C. Soghoian*, 'Exclusive: The next Facebook privacy scandal', CNet News, 23 January 2008, available at: *www.cnet.com/8301–13739_1–9854409–46.html*.

24 Ofcom 2008, supra note 1, p. 53. Also pointing to the importance of social pressure, *Utz & Krämer* 2009, supra note 1.

25 According to Art. 12 of the Data Protection Directive, data controllers are obliged to notify third parties to whom the data have been disclosed of any rectification, erasure or blocking, unless it proves impossible or involves disproportionate effort.

Apart from the question of what "appropriate technical and organizational" measures are and if e.g. simple password protection is already sufficient, securing personal profiles against unauthorized access of the data they contain requires that the operator of the site provides for these possibilities. In practice, most sites probably will do so. Yet the fact remains that users are dependent upon the general architecture of the site. Moreover, passwords may protect to a certain degree against unauthorized access, but not e.g. against alteration, loss and destruction. It is only in the power of the site's operator to implement more powerful privacy enhancing technologies. In other words, the extent to which amateur users can be expected to comply with provisions in data protection law also depends on the extent to which users can expect support from and cooperation with the operators of SNSs (see extensively section IV. below).

Finally, and more fundamentally, some provisions in existing data protection law probably should not be applied to individual users, at least not in certain circumstances. An example of such circumstances could involve situations in which a strict application of data protection obligations unduly restricts users' right to freedom of expression as protected by Article 10 of the European Convention on Human Rights. Note that Article 9 of the DP Directive specifically calls on the member states to reconcile their data protection laws with freedom of expression.[26] Article 9 DP Directive modifies the applicability of the stringent norms for the processing of sensitive data, the information to be given to a data subject and the rights of data subjects if this would otherwise inhibit journalist purposes, as well as artistic and literally expression.

3. Media Exemption

To the extent that the publication of personal data on SNSs serves journalistic, artistic or literally purposes this so-called media exemption could apply.[27] Notably, SNSs are quite successful as platforms for amateur writers, bands or photographers. MySpace, for instance, has attracted millions of musical groups that promote their artistic creations through the site. Many politicians and non-governmental organizations are active users of SNSs. They use SNSs to connect to internet users and use the platform's capacities to facilitate amateur user contributions in public campaigns and debate. Furthermore, SNSs have also become an important means for people to receive (and comment) on the news.[28] On SNSs, public debate blends with the personal. Comments and discussion about the prime minister appear next to tagged holiday photos. Together, SNS users create a filter for their daily input of news and entertainment, ranging from content of a purely personal nature to content that is typically covered by traditional news outlets. SNS might be 'new' media, they are media nonetheless, and its users are its main contributors. It is clear that data protection law, if applied to the online activities of natural persons, will have to take account of these realities to prevent unwarranted restrictions on the communicative freedoms of individuals.

4. Result

To sum up, the law burdens SNS users with a set of data protection obligations that either go beyond their personal expertise and/or financial and technical capacities or do not fit the SNS context. Apart from the examples from existing European Data Protection law that were discussed here, national data protection laws may impose additional, different or more precise obligations.[29] More awareness among judges and policy and lawmakers is accordingly needed regarding the specific situation of amateur data controllers. To the extent that new, more specific obligations geared to the conditions on SNSs arise in the form of formal law-making or self and co-regulation (e.g. with regard to the processing of the personal data of children[30] or technical privacy design[31]), this might be an opportunity to take amateur data controllers more consciously into account.

Another question that requires more attention and research is whether the present "one-size-fits-all" approach in data protection law takes sufficiently into account the heterogeneity of SNS users (and if not, how it is possible to differentiate in (the application of) data protection law). Among the adult participants of SNSs, huge differences dictate the scene. There are users with 10 and users with 3000 friends and their type of SNS usage varies wildly. In addition, a substantial part of users on SNSs is underage. Is it appropriate, desirable and realistic to expect from them, or their unsuspecting parents, the same level of care and conformity as from adult users?[32]

IV. Sharing Burdens

Acknowledging that individual users can be data controllers for the data in their personal profiles raises another question, namely about the division of responsibility with the providers of SNS services. Interestingly, most major platforms do not consider themselves to be legally responsible at all for the content in personal profiles. They argue that all profile information is made available by users, voluntarily. For example, MySpace states:

> "Because the Member, not MySpace, determines the purposes for which Profile Information is collected, used and disclosed, MySpace is not the data controller of Profile Information that Members provide on their profile."

Similarly, Facebook instructs its users:

> "If you collect information from users, you will obtain their consent, make it clear you (and not Face-

26 Art. 9 DP Directive provides that "Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."

27 In this sense also the Article 29 Data Protection Working Party (2009), supra note 7, p. 6.

28 See e.g., *Mike Melanson*, 'Facebook Drives 3X Traffic to Broadcast Than Google News', ReadWriteWeb, 1 March 2010.

29 See recital 22 of the Data Protection Directive.

30 See e.g. Safer Networking Principles for the EU, 10 February 2009, available at *http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf*. See also, United States State Attorney Generals and MySpace, Joint Statement on The Key Principles of Social Networking Sites Safety, 14 January 2008, available at *www.mass.gov/Cago/docs/press/2008_01_14_myspace_agreement_attachment1.pdf*.

31 See e.g. the Safer Networking Principles for the EU, supra note 30.

32 The issue of the underage SNS users raises a host of legal questions, for example whether underage users can meaningfully "consent" without the consent of their parents.

book) are the one collecting their information, and post a privacy policy explaining what information you collect, and how you will use it."

Sometimes, users are not only held responsible for their own activities, but also for the activities of their friends: As Netlog puts it:

> "As a user, you assume complete responsibility and liability, without protest, for any information you publish and/or any activity in which you engage on or via your profile. You are not only liable and responsible for the items you publish on your page, blog, photo album etc., but also for the comments and responses that others publish on your page. You can remove undesired content easily."[33]

Note in this context that according to the Article 29 Working Party the terms of a contract are not decisive when defining who has the responsibilities of a data controller. Otherwise this would, as the Working Party clarifies, *"simply allow parties to allocate responsibility where they think fit"*.[34] This view is supported by European law and its conceptualization of data protection as a fundamental right. Although the DP Directive does not explicitly clarify the mandatory character of its provisions, it is generally assumed that the DP Directive has created a legal regime for the lawfulness of personal data processing through a body of mandatory obligations and non-waivable rights.[35] In this regime, consent and contract play an important role, in particular in the relationship between data controllers and data subjects. However, the substantive rights and obligations, as well as their allocation, remain based on the DP Directive and are not affected by contract. Notably, in the context of the legal relation between SNS providers and users, the DP Directive grants rights to and imposes obligations related to the interests of third parties. These, in particular, cannot be affected by a contract between other parties.

On a more general note, there is a tendency in today's media law and policy to adopt a more functional approach when approaching questions of accountability and responsibility for compliance with the existing regulatory framework and give also weight to aspects such as the respective business model, actual (economic) benefits and, more pragmatically, the ability to solve a problem most effectively and efficiently.[36] As the Article 29 Working Party rightly has pointed out, SNS providers do retain a considerable amount of control about the purpose and means of data processing on SNSs, through the way SNSs are structured, the "basic" services they offer and also as a result of their business model and monetization strategies. The Working Party concluded that already for this reason SNSs must be considered to be data controllers, irrespective of the status of users.[37]

The cited provisions demonstrate at the same time the dilemma SNS providers and users are confronted with: the entire business model of MySpace and the other Social Network Sites is built on users placing personal content on their own and on each other's profiles. Accordingly, an argument can be and is made that because SNSs provide specific means and facilities to engage in privacy risks and infringing activities and because platforms, to some extent, may even benefit from such activities, it is not acceptable that SNS deny all responsibility for what happens on users' profiles. On the other hand, it is virtually impossible and equally invasive for SNSs to supervise and control all the activities of their users. Many privacy problems on SNSs are user generated (see above) or could be at least more effectively or cost-efficiently avoided or addressed by users. Accordingly, it seems only reasonable and adequate to place some responsibility for the lawfulness of actions on SNSs on the users themselves. However, SNS users are only to a limited extent able to guarantee that the processing of personal data on their profiles complies with data protection law – because they lack the legal knowledge, because the law does not fit the situation of SNS users or because they lack the technical and organisational resources. The only workable solution to the dilemma seems to be a well-designed model of "shared responsibility" or a division of tasks to guarantee the fairness of the processing of personal data on users' profiles.

In its opinion 1/2010 the Working Party does acknowledge that in complex systems with multiple actors the division of responsibilities for the processing of personal data may not be straightforward, specifically mentioning the case of social networks as an "interesting scenario". According to the Working Party it is for the actors who exercise joint responsibilities to distribute and allocate obligations and responsibilities among them, in a transparent and effective way that ensures full compliance.[38] In practice, the relationship between SNS providers, users and their friends will be characterised by a lack of individual negotiation (power) on the side of users, as well as considerable asymmetries in knowledge and resources – a situation that further complicates the proper allocation of responsibilities. Moreover, the situation of users and their friends will be to a considerable extent influenced by (possibly diverging) social norms, uses and pressure.

1. Information

In order to comply with their duties as data controllers, users need two kinds of information: practical information about the potential security and privacy risks on SNSs and legal information. Accordingly, Principle 1 of the European Safer Social Networking Principles[39] demands that SNSs "create clear, targeted guidance and educational material designed to give children and young people the tools, knowledge and skills to navigate their services safely". The Art. 29 Working Party also recommends that "SNS providers provide adequate warnings to

33 Netlog, Terms and Conditions, available at: *http://en.netlog.com/go/about/legal/view=general.*

34 See Article 29 Data Protection Working Party 2010, supra note 5, p. 11.

35 See e.g. *Lucas Bergkamp, European Community Law for the New Economy*, Antwerp, Oxford and New York: Intersentia, 2003, p. 123. For a discussion of the possibility of leaving more room for contractual arrangements and waiving of data protection rights, see *Colette Cuijpers*, 'A Private Law Approach to Privacy; Mandatory Law Obliged?', SCRIPTed, Vol. 4, nr. 4, 2007.

36 For an extensive discussion, see *F. Le Borgne-Bachmidt, N. Helberger, S. De Munck, S. Girieud, M. Leiba, S. Limonard, M. Poel, L. Guibault, E. Janssen, N. van Eijk, C. Angelopoulos, J. van Hoboken* and *E. Swart*, 'User-Created-Content: Supporting a participative Information Society', Report for the European Commission, DG Information Society, December 2008, p. 227 subsq. (with further references), available at: *http://ec.europa.eu/information_society/eeurope/i2010/docs/studies/ucc-final_report.pdf.*

37 Article 29 Data Protection Working Party 2009, supra note 7, p. 5.

38 Article 29 Data Protection Working Party 2010, supra note 5, p. 24.

39 This is an example of self-regulation, which has been endorsed by most major SNS platforms in Europe. Safer Social Networking Principles for the EU, 2009, supra note 30.

users about the privacy risks to themselves and to others when they upload information on the SNS". However it also sees a role of SNS operators in providing users with legal information/education, namely by advising them that a) uploading information about other individuals can infringe their privacy and data protection rights and b) that uploading pictures and information about other individuals requires prior consent.[40] In the Social Networking Principles, SNSs have committed to provide users not only with information about what constitutes inappropriate behaviour, but also about the legal consequences of such behaviour.[41] Moreover, the principles require that providers "should explore other ways to communicate this information outside of the Terms of Service."[42]

In other words, simply and generally informing users that they are to "assume complete responsibility and liability" or to develop their own privacy policies is not enough. Instead, this article suggests that SNSs must also provide users with guidance, the necessary organisational and technical support and functional legal expertise. The call is for platforms to provide users with more detailed information and yes, even to educate them. The challenge for SNS is to do so in a way that can be understood and respected by users – as well as to do so in a "social network friendly" way. So, for example, instead of pointing users to the need of drafting their own privacy policy, platforms could provide users with a model privacy policy or a 'privacy policy wizard tool'. Lengthy explanations in obscure legal English, Dutch or other language could be replaced or complemented by a concise virtual "your obligations as a data controller" tour, manual or video course. And instead of only informing users that they need to obtain the consent of others before publishing their images or videos, platforms could design build-in mechanisms to support them in this task. This is at least the opinion of the Article 29 Working Party that makes very concrete design suggestions that go beyond purely informing consumers about their obligations. The Working Party suggests, for example, that SNSs could introduce tagging management tools that indicate if a user's name appears in a photo or set expiration times for tags that have not received consent by the tagged individual.[43]

2. Settings

Some platforms have already developed a number of interesting examples of technical and organisational measures that support users when they exercise their responsibilities as data controllers and respectively prevent them from abusing the service.[44] As a minimum standard, most sites enable access control technologies so that users can control who has access to all the information on their profiles (including information about friends) and prevent this information from being "published" to a broader audience. Most sites also allow users to prevent the listing of their profile in search engines. For example, Facebook users can decide whether they allow or do not allow search.[45] Meanwhile, more differentiated and intelligent solutions are being developed. Most of these applications concentrate on enabling users to protect their own information from unwanted circulation and re-use, rather than managing other people's information.[46]

One example is from Facebook, a company that is usually cited for its privacy sins rather than for its privacy virtues, but that has, in part due to the pressure to better protect users' privacy, also developed a number of privacy protection solutions. Facebook users can select the privacy settings for each post by simply clicking on an icon and choosing whether that particular piece of information can be shared with everyone, with friends of friends, only with friends or only with certain friends (with the ability to list friends) or only viewed by the user his/herself. This tool allows users to manage who has access to certain personal information, thereby reducing the risk of leakage and abuse. Optimistically speaking, this solution could also be seen as an example of a more innovative attempt to gear solutions towards network-centric theories of privacy. It acknowledges that certain types of information is more likely to spread broadly (also against the will of their owner) than others.[47] Moreover, it takes into account that one element of privacy is to determine the context in which personal information is being used and shared.[48]

A more fine-grained level of control is offered users by Clique. Clique is the prototype of a privacy enhanced Social Network Site developed under the PrimeLife project. Clique's settings enable users to identify different spheres and identities and to choose for each identity the corresponding audience. Through the architecture of the site, users can customize their audiences and to control who can access which information.[49]

Not only Facebook but Facebook's users as well have developed technical solutions to protect their privacy. One example is a Facebook application called "Respect my Privacy" that develops a Creative Commons-like system of classifying and labelling usage restrictions (non-commercial, non-depiction, no-employment, no-financial, no-medicine).[50] A somewhat different and

40 See Article 29 Data Protection Working Party 2009, supra note 7, p. 7.

41 See Principle 1 of the Safer Social Networking Principles for the EU, supra note 30.

42 *Ibid.*

43 See Article 29 Data Protection Working Party 2009, supra note 7, p. 7–8.

44 See also Pew Internet, Reputation Management and Social Media How people monitor and maintain their identity through search and social media. Report, May 2010, p. 4 subsq., exploring how internet users use settings and more generally a site's architecture to protect their privacy, available at: *www.pewinternet.org/Reports/2010/Reputation-Management.aspx*.

45 See The Facebook Blog, 'New Tools to Control Your Experience', 9 December 2009, available at: *http://blog.facebook.com/blog.php?post=196629387130*. The default setting is on allowing search by search engines and, when opting out, users get a warning that opting out will make it more difficult for their friends to find them.

46 See also Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels, 18 March, 2010, extensively elaborating on the benefits of privacy by design, available at: *www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf*.

47 *L. Strahilevitz*, 'A Social Network Theory of Privacy', John M. Olin Law & Economics Working Paper No. 230, 2004, available at: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=629283*.

48 For a discussion see *D. Solove*, *The Future of Reputation*, New Haven and London: Yale University Press, 2007, p. 165, available at: *http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text.htm*; *W. Hartzog*, 'The privacy box: A software proposal', First Monday, Vol. 14, No. 11, 2009; *T. Kang* & *L. Kagal*, 'Establishing Social Norms for Privacy in Social Networks', MIT CSAIL, Cambridge (MA), United States, 2009, available at: *http://dig.csail.mit.edu/2009/Papers/ISWC/rmp-ws/paper.pdf*.

49 For more information about Clique, see Leenes 2009, supra note 1, and the PrimeLife Project: *www.primelife.eu/results/opensource/40-clique*.

50 Respect my Privacy application, *www.facebook.com/apps/application.php?id=10637134047*. See also *T. Kang*, Respect my Privacy, Master's thesis in Electrical Engineering and Computer Science, MIT, 2009,

more academic proposal is that of the "Privacy Box", which to the knowledge of the authors has not yet been implemented. The Privacy Box is an application that supports the conclusion of binding confidentiality agreements between users.[51]

An example for a technological solution that is designed to manage, not infringe on other people's privacy is Flickr's tagging tool. In Flickr, users can indicate preferences as to who can add them to a photo (only you, friends, family, contacts, any Flickr member). If one's name is added to a photo, the added person will be able to see the photo, irrespective of the privacy settings of the person who uploaded the photo. Flickr also provides each user with an overview of the photos in which he or she is marked, together with the possibility of removing his or her name from all these photos. Once removed, no one will be able to add that person to those particular photos again.[52]

3. Conflict Management

Acknowledging that individual users can be data controllers and enabling friends to exercise their rights of fair processing of their personal data are two different things. In practice many of the conflicts between friends involving the exchange of personal data will be handled informally. In the ideal scenario, over the course of time social norms will develop and in some instances an increased and shared sense of confidentiality might come to rule relationships between friends.[53] SNSs provide a fascinating field for the study of not only user-created privacy problems, but also user-created solutions. Hence, an interesting topic for further law and policy studies could be the role of SNSs[54] and of the law[55] in fostering the development of such rules and promises of confidentiality. Already now, many SNSs draft codes of conduct or guidelines for users on how to behave on their networks. Having said this, the definition of cultural and social norms in online social networks is still in its infancy.[56]

Until then, and in the event that "things get nasty", friends do have a number of legal rights (e.g. the right to information, the right of access, the right to demand rectification, erasure or blocking of certain data), which they can exercise, at least in theory, also in relation to amateur data controllers (see section 4). In practice, however, it can be extremely cumbersome for friends to exercise their rights. Reasons can be that the data subject is no (longer) connected to the amateur data controller (e.g. because he has been de-friended), the amateur data controller hides behind a virtual identity, or simply because he does not respond to individual requests.

In these situations, there is little that data subjects can do to handle their rights. A contractual relationship between users generally does not exist. As mentioned earlier, some SNS do formulate certain rules on how to behave on SNSs (including rules on how to respect the privacy of other users) and reserve the right to sanction violations of these terms, for example through the termination of the service. These terms of use only apply between users and SNSs, not between individual users. This is why friends, too, depend upon support from and cooperation with the website.

Existing conflict management mechanisms on SNSs can be roughly distinguished in complaint procedures and self-help, whereas complaint mechanisms clearly dominate. All platforms reviewed offer the opportunity to complain to the provider of the service about the unwanted or unlawful behaviour of others. The platforms vary in ease of filing a complaint (while e.g. Netlog requires an email, MySpace, Facebook and Flickr have Report Abuse buttons, making it somewhat easier for users to make a complaint). Few of the report abuse buttons offered specifically mention privacy problems. Privacy problems are commonly and more generally referred to as violations of community guidelines or terms of use (e.g. Flickr) or users can only flag content as inappropriate. An important tool to facilitate compliance with written (but also unwritten social) data protection rules could be standard forms that allow users to object specifically to the way certain personal data is being processed or to require the rectification, erasure or blocking of certain personal data because they are e.g. incomplete or inaccurate. Ideally, the form would enable friends to direct a standardised complaint not only against the operator of the platform, but also against the user. These forms would need to be accompanied by effective procedures that guarantee that the interests of all parties (platforms, users and friends) are respected, including the users' fundamental freedoms, such as freedom of expression (see section 4).

More generally, it could be interesting to experiment with various forms of user-executed control and sanctioning of privacy-infringing behaviour. The scarce existing research suggests that, for some fields of law, user-executed control and sanctioning could potentially be very powerful, but that it also bears considerable risks for individual rights and the public order, including wrongful accusations, disproportionate punishing and lasting damage to a person's reputation, business or profession.[57]

available at: *http://dig.csail.mit.edu/2009/tedkang-thesis/Ted%20Kang%20-%20MEng %20Thesis.pdf*. Other potentially privacy enhancing technologies which have been written by users for users are the Privacy Mirror ("This application shows you what 3rd party developers can see in your profile based on your current privacy settings."), available at: *www.facebook.com/privacymirror*, and the Privacy Protector ("Privacy Protector is a Facebook application that creates a new, secure information section in your profile. Information in the secure section is hidden by default, so it cannot be stolen!") available at: *www.facebook.com/apps/application.php?id=11721128773*.

51 *Hartzog* 2009, supra note 50.

52 See *www.flickr.com/account/prefs/photospeople/?from=privacy*.

53 See *Solove* 2007, supra note 50, p. 173, defining confidentiality as "an expectation within a relationship: When we tell others intimate information, we expect them to keep it confidential." Solove, however, also points out that, at least US law holds little regards of (oaths of) confidentiality among privates, ibid, p. 174–176.

54 See e.g. *Hartzog* 2009, supra note 50. See also *Kang* & *Kagal* 2009, supra note 50, suggesting a "Respect My Privacy (RMP) framework".

55 *Solove* 2007, supra note 50, p. 176: "The law should provide a remedy for gossip when it is spread widely or permanently".

56 See e.g. *Kate Carruthers*, 'Social networking & social norms', 17 March 2009, available at: *http://katecarruthers.com/blog/2009/03/social-networking-social-norms*. See also *D. Fono* & *K. Raynes-Goldie*, 'Hyperfriendship and Beyond: Friends and Social Norms on LiveJournal', in *M. Consalvo* & *C. Haythornthwaite* (eds.), Internet Research Annual Volume 4: Selected papers from the association of Internet Researchers Conference. New York: Peter Lang, 2006, available at: *http://k4t3.org/publications/hyperfriendship.pdf*.

57 See e.g. *M.F. Schultz*, 'Fear and Norms and Rock & Roll: what Jambands Can Teach Us about Persuading People to Observe Copyright Law', Berkeley Technology Law Journal, Vol. 21, p. 651, 2006, available at: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=864624*; *B. Balázs*, 'The Club model of cultural consumption and distribution', Working Paper, Draft, Last Revised 7 April 2007, available at: *www.warsystems.hu/wp-content/uploads_bodo/club_model_proposal.pdf*; *E. Fauchart* & *E.A. von Hippel*, 'Norms-Based Intellectual Property Systems: The Case of French Chefs', MIT Sloan Research Paper No. 4576–06, January 2006, available at *http://ssrn.com/abstract=881781*; *L. Strahilevitz*, 'Charis-

To sum up, some SNSs try to contract away the legal responsibility – as bestowed upon them by the DP Directive – for their role in the processing of personal data and the privacy-sensitive activities of users in particular. There is a growing perception that SNSs and users must be held at least jointly responsible for the safety of information on personal profiles and that more attention should be given to the way responsibilities are allocated between them. In practice, it can be observed that SNSs actually will take one measure or another to support users in complying with their functions as data controllers, either by providing them with the necessary factual or legal information or by technical and organisational measures and mechanisms of conflict solving. What is missing, however, is a more concerted, systematic approach to joint responsibility and shared burdens. The absence of such a comprehensive approach to user-created privacy problems on SNSs could be at least in part the result of a lack of economic and legal incentives (or threats) for SNSs to tackle this thorny and unpopular issue. More legal certainty is needed about the way in which SNS platforms, users and friends are jointly responsible for the safety and confidentiality of profile information and the extent to which SNS platforms are obliged to assist amateur data controllers in keeping their own and their friends' profile information safe. Also, a discussion is needed as to what extent provisions in the terms of use that deny any responsibility for the safety of personal profile information must be considered "unfair" under general contract law, at least in situations in which platforms do not provide users with the tools to guarantee an adequate level of safety themselves.

V. Conclusions

Amateurs who do not protect their profiles against unauthorized access, who pride themselves on a large number of friends, who allow their profiles to be "searchable" (or who do not know how to disable that function), who use SNSs, as many do, in order to stay in touch with professional contacts or as stepping stones for (semi)professional activities are, in all likelihood, data controllers. This article has explained why the household exemption needs to be interpreted restrictively in the SNS context.

This may be an inconvenient truth not only for amateur users, but also for policy makers. It means that a substantial part of SNS users is fully responsible for observing the provisions of national data protection laws. Few users will be aware that they are posting and poking under a legal Damocles sword that is ready to strike in the event that things go wrong. And while it may be appropriate and even beneficial to impose some of the legal safeguards on individual users, other provisions are ill-fitted and out of proportion when applied to the amateur. This is because existing data protection law has been designed to address (large) commercial entities and public authorities, that process personal data as part of their professional routine. It is not prepared for a situation in which individual users assume activities that, so far, have been reserved for professional data controllers and in which the processing of personal data is not any longer a byproduct of commercial activities, but a purpose in itself.

For policy makers this means that they need to take the amateur user into account and reconsider the universal application of data protection law to professional and amateur data controllers. When so doing, it would also be important to carefully balance the privacy interests of friends with the freedom of expression claims of users that process personal data. The current regulatory framework, if applied to individual internet users, could lead to undue interference with their communicative freedoms. Finally, more attention is needed for the just allocation of responsibilities for the processing of profile information between users, friends and platforms.

Legal responses are neither the only possible nor necessarily the most preferable responses. This paper has made some suggestions as to how joint responsibility between users and platforms can be given concrete form through the design choices of SNS platforms themselves. The lack of legal pressure on SNSs can act as a further disincentive for platforms to tackle a thorny and naturally hugely unpopular problem.

matic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks', 89 Virginia Law Review 2003, available at: *http://ssrn.com/abstract=329700*. *Solove* 2007, supra note 50, p. 76.

Wiebke Baars/Roland Broemel

Keyword Advertising – Settled Points and Open Questions

A closer look at the emerging judicial approach in the European Union

The permissibility of optimizing online advertising by using third parties' trade marks as keywords is one of the topics that have been currently discussed within the last years and which have been subject to several partly contrasting decisions in a number of European countries. Following the submissions of several European courts concerning Google's Ad-Word system the European Court of Justice (ECJ) has laid down the criteria under which keyword advertising constitutes a trade mark infringement. The limits of keyword advertising set by third party trade marks are, however, subject to case-to-case decisions of the national courts. Though the ECJ has established that using trade marks as keywords for advertising constitutes a use in the course of trade in relation to goods or services, the question whether there is an adverse effect on the functions of the trade mark basically depends on an assessment of the link between the results of the search engine and the advertisement optimised via the keywords. Therefore, the criteria established by the ECJ are subject to precision by the national courts.

▷ Dr. Wiebke Baars, LL.M. (UCL)/Dr. Roland Broemel, maitre en droit, Hamburg. Further information about the authors at p. 128.