Social networking: a conceptual analysis of a data controller

Rebecca Wong

Introduction

> *'You want to be social with your friends, but now you're giving 20 guys you've never met vast amounts of information from your profile. He said "that should be troubling to people."'*[1]

The article is intended to revisit the definition of a 'data controller' as laid down under the Data Protection Directive 95/46/EC. The main thesis of the author is that within a social networking environment, it is becoming easier for individuals to be brought within the scope of a 'data controller.'[2] The discussion will take into account the recent Article 29 Data Protection Working Party opinion on social networking, which has recently clarified the extent to which social network providers and users are considered 'data controllers.' If one examines the traditional legal definition of a data controller within the Data Protection Directive 95/46/EC:

> *'A natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.'*

The problem that arises is that the Data Protection Directive 95/46/EC was drafted at a time when the internet was still at its infancy. However, with the second generation of the internet, often loosely termed as web 2.0,[3] it is becoming possible that *anybody* can be brought within the scope of the broad definition of a 'data controller', leading to the question over how the data protection framework is going to be enforced (should litigation between one or several individuals arise). The article will take the following structure. I will consider the first issue – who constitutes a 'data controller' – within the data protection framework in the light of the recent Article 29 Data Protection Working Party opinion on social networking. This will be followed by a discussion of the legal definition of a 'data controller' and the implications arising out of this definition; the dilemmas raised under the data protection framework as applied to SNS. I will then consider the views of the data protection authorities, followed by a discussion into the consequences of web 2.0 technologies within a SNS before drawing my conclusions on this analysis.[4]

Dilemmas

As the breadth of the definition of a 'data controller' is wide enough to include any individuals who post information about others on the internet, the question is why does this matter and what, if any, are the implications? The Directive was originally intended to regulate activities of organisations in processing personal data, and social networking presents a different dimension to the problem in the sense that one is dealing with users (who have multiple roles both as 'data subjects' and as 'data controllers') and post information about others (be they friends, colleagues and associates). The main questions to address in a social networking environment are:

- Who are our users/data subjects?
- What are the obligations for data controllers laid down under the data protection laws?
- How easily would information about others be circulated and would there be the opportunity to remedy the damage?

According to a recent study by the International Working Party on Telecommunications, the likely threat that may arise by posting a user's profile in a social networking environment is the rise of identity theft. In a recent press release titled 'New front in the battle against identity theft':

> *'Millions of young people have made themselves vulnerable to identity theft as well as putting their future academic and professional prospects at risk by recklessly posting personal information on the internet, Britain's privacy watchdog warns in a report published today.*
>
> *'The report's findings will add to increasing fears about the unchecked growth of personal information held in Britain and the way it is protected after a security blunder at HM Revenue & Customs in which highly sensitive details belonging to 25 million people were lost in the post. Now, in a far-reaching study of the internet behaviour of young people, the Information Commissioner's Office (ICO) says that 4.5 million web users aged between 14 and 21 could be vulnerable to identity fraud because of the carefree way they give up information on the internet, especially when visiting social networking sites.'*[5]

Similarly, 'Watchdog', the BBC consumer programme, recently created a Facebook page with a cartoon picture of a woman in her 20s and invited 100 random people to join as her friends. The programme was able to show how the identities of the friends were stolen and details used to open an online bank.[6]

Whether the application to users of SNS would be strictly enforced by data protection authorities or individuals when something goes wrong is not yet certain. The Article 29 Data Protection Working Party's opinion has taken the view that in most instances individuals who use a networking site for private purposes would fall outside the scope of the Data Protection Directive.[7] There are limited circumstances when individuals could still fall within the category of 'data controller' even if they do not use the social networking site for private purposes.

At the time of writing, one notable case that reached the UK courts concerned a user who brought legal action against his former friend for posting a false profile on Facebook. The case is significant for clarifying the extent to which users can bring a legal action. In *Applause Store Productions Ltd and Anor v Raphael*[8] the court found for the claimant on the grounds of 'misuse of private information':[9]

> *'As far as the tort of misuse of private information is concerned, I accept Mr Firsht's evidence that it caused him, a very private person, great shock and upset. The information which has been conceded to be private, or which I have held in the private annex to this judgment to be private, related to his supposed sexual preferences, his relationship status (single or otherwise), his political and religious beliefs, and his date of birth. It seems to me that the most important information is that which relates to his supposed sexual preferences.'*[10]

There was no question that some of the statements made in the Facebook profile were defamatory, but it is the tort of misuse of personal information that is of interest for the purposes of this article. If one is permitted to extend this further to a data protection framework, the posting of a profile is also construed to be 'processing' of personal information within section 1 of the Data Protection Act 1998 and may even constitute the processing of 'sensitive' personal information within section 2 of the Data Protection Act 1998. With social networking websites, it is becoming easier for users to post comments that portray individuals in a different light and could potentially be defamatory. This is a separate legal ground from data protection and will not be discussed further in this paper.

Whilst Facebook has adopted sophisticated technological measures for the user to protect their privacy settings, it does not deal with user etiquette nor with personal information or individual's profiles that get out of control. It is possible for Facebook to simply remove the profile of the user or enable the user to delete this. Whether they would be operating as a censor is another question. Simple steps to inform user etiquette and peer pressure to ensure that this forum is not misused would go a long way.

Who is a 'data controller'?

Whilst the paper does not call for a radical overhaul in the traditional definition of a 'data controller',[11] it does call for a rethink in the approach by legislators and even the judiciary about the likelihood of lawsuits that may be brought by individuals on the basis that other individuals were processing personal information based on the legal definition of a 'data controller.'[12] This has already happened with one case which was successfully brought by one individual in the UK for posting a false profile of the user. The issue of a 'data controller' is likely to be a question of fact as laid down under the DPA 1998 (*Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47).

'The issue is whether the broad interpretation of a "data controller" is likely to lead to a flood of cases involving the misuse of personal information on social networking websites. How do we quantify and identify who are the data controllers?'

At the time of writing, the Article 29 Data Protection Working Party had issued a recent opinion that users would generally be covered under the article 3.2 private purposes exception, but could, in limited circumstances have data protection responsibilities, if they fall outside the scope of the private purposes exception. An example given would be where the SNS was used as a collaboration platform for a company[13]. The distinction between private use of a social networking site and other uses can be very difficult to draw and therefore, a rigid application of the Directive is not what is called for, but sensible application by the data protection authorities.

Some of the implications that arise for Data Protection Authorities are that if individuals are viewed as 'data controllers'[14] then:

(1) **Data protection principles would need to be followed** – this includes processing personal data fairly and lawfully and ensuring that it does not exceed what is required. Requiring *all* individuals to abide by the data protection principles on a social networking would be difficult to police and enforce. It also demonstrates a specific problem about the data protection framework in fitting this to new uses. Therefore, strict compliance would need to take account of practical realities.

(2) **Regulators/data protection authorities** – the likelihood of opening the floodgates principle. The courts should not be inundated with claims that individuals' images/comments about other individuals have not been inappropriately misused on social networking websites. Other than users complaining before their social network providers, there should also be an alternative dispute resolution process, such as an independent arbitrator that will determine the use of social networking disputes whereby parties agree that decisions by the arbitrator would be binding and the law to be applied.

(3) **Use of the exemptions** – understand that the exemptions should be clearly, narrowly interpreted and applied. In particular, article 9 of the Data Protection Directive 95/46/EC to social networking websites is likely to be of interest – is the profile used for 'journalistic purpose or not?.' There have been relatively few cases determining the application of article 9 of the Data Protection Directive. However, in the recent significant case of *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy*,[15] the European Court of Justice ('ECJ') took the view that data taken from documents that were in the public domain would fall within the exemption of personal data carried out 'solely for journalistic purposes.' The ECJ also took the view that this would be a matter for the national courts to decide and would involve a balancing act. Section 32 of the UK Data Protection Act 1998 provides a narrow test on the use of the journalistic purpose exemption. It takes a three pronged approach to determine whether processing was intended for journalistic purpose, namely:

> *'(a) …with a view to the publication by any person of any journalistic, literary or artistic material;*

(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and

(c) the data controller reasonably believes that, in all the circumstances, compliance with (statutory provisions) is incompatible with the special purposes).'

Whilst this does not suggest that section 32 cannot entirely apply to social networking websites, it would only do so in the limited circumstances described above. Although the application of section 32 of the DPA 1998 to SNS is still untested in the UK courts, the Court of Appeal decided in the case of *Campbell v MGN Ltd*[16] that section 32 of the Data Protection Act was to be given their natural meaning and would apply before and after publication. The Court of Appeal also took the view that section 32(4) and (5) were purely procedural aimed at providing for the stay of proceedings against a publisher until after publication.[17]

The other exemption that may override the protection of an individual's personal privacy is article 13(1)(g) of the DPD on the protection rights and freedoms of others. To date there have been no cases in the UK to decide on this, so it is not entirely certain how this will apply in practice.

Ultimately, the consent of the individual will be key to whether he or she would like her personal information be used by others and aggregated to form a personal profile. The key would be to understand limitations of regulation in its application to SNS and ways in which individuals ought to protect their own identity.

Data Protection Directive 95/46/EC and its application to SNS

The section below will consider, in brief, the application of the Data Protection Directive to SNS. As the Data Protection Directive is applicable to social networking users as 'data controllers', the main provisions of the Directive will therefore apply (not exhaustive):

(1) Data protection rights and obligations as laid down under articles 7 and 8
(2) Rights of the data subjects under article 10

It is unclear whether the Directive (or national data protection laws) would be enforced in the strict sense as personal information is readily available on SNS. Secondly, users have consented to have this information given to users. However, there is a difference between data given for original purposes and data used for secondary purposes. It is unlikely to satisfy the consent requirements where third parties use the profile of individuals without their permission.

Whilst the Article 29 Data Protection Working Party has indicated recently how article 3.2 of the Data Protection Directive should be applied to a social networking environment,[18] the *Lindqvist*[19] decision by the ECJ is unlikely to avail for individuals who wish to benefit from the private purposes exemption for posting personal information about others in the online environment if it can be shown that the profile is easily accessible to anybody and was not used for purely private purposes.[20] In Lindqvist, L had created a web page containing personal details (including the interests and hobbies) of some of the members of the parish church, and also mentioned that one of the members had injured her foot. The Swedish court took the view that she had contravened the PDA 1998 and subsequently fined her. The questions brought before the ECJ under an article 234 preliminary ruling were whether the information about the individuals placed on the web constituted personal data, and secondly whether this constituted the transfer of personal data contrary to article 25 of the Data Protection Directive, which prohibits such transfer without the assurance that the recipient country had adequate safeguards on data protection in place.[21] The ECJ interpreted the scope of article 8 of the Data Protection Directive 95/46/EC widely,[22] and had held that article 3.2 would be unable to avail on the basis that information was available/accessible to anyone on the internet (no discussion was made by the ECJ of restricting access using intranets).

Article 4 of the Data Protection Directive applies to user-generated content based within the EU. Article 4(1)(a) of the Data Protection Directive provides that this Directive (or corresponding national data protection laws implementing the Data Protection Directive) apply to activities of an establishment of the controller on the territory of the Member State and/or article 4(1)(c) uses equipment to process. For example, in the example of MySpace, there are potentially two data controllers. Firstly, there is MySpace that holds the personal information of their users, and secondly there are the users themselves. It is established that MySpace has an office in the UK. They would be likely to be construed as data controllers within section 5(1)(a) of the DPA 1998. A data controller is established in the UK and the data is processed in the context of that establishment. The alternative would be if MySpace uses equipment to process personal data within section 5(1)(b). If section 5(1)(b) applies, then the data controller (MySpace) would be required to nominate a representative within the UK.[23] However, reading through their privacy policy, they draw a dividing line when they are data controllers or not:

'MySpace determines the purposes of collection, use and disclosure of the Registration Data you provide and, as such, is considered the data controller *of this information. 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 (emphasis added).'*[24]

Users of their profiles are considered as 'data controllers', but as MySpace also has a UK MySpace webpage which collects the profiles of individuals in the UK they would still governed by the UK Data Protection Act 1998.

Article 13 of the Data Protection Directive 95/46/EC restricts the scope of the obligations and rights provided for in articles 6(1), 10, 11(1), 12 and 21 of the DPD when such a restriction constitutes a necessary measure to safeguard (a) national security (b) defence (c) public security (d) prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions (e) an important economic (g) *protection of the data subject or of the rights and freedoms of others* [my emphasis].[25] It is this final category which is likely to apply, but to date there have been no cases to clarify the breadth of this.

The general thrust of the argument is that if the data protection framework is to be applied effectively, then it will need to recognise that the difficulties provided under the framework cannot be solved instantaneously. Any changes to the European data protection framework would need to begin at a European level. In the meantime, the application is likely to lead to major questions about the relevance of the framework to social networking environment.

Work of the Data Protection Commissioners

How have the Data Protection Commissioners responded to the growing rise of the use of SNS, and what, if any guidelines have been published? Several Data Protection Commissioners have already issued guidelines on the use of SNS, but these take a limited and cautious approach about users posting information rather than recommending a remedial effect when SNS goes wrong. Even if SNS is not discouraged and has been seen to have a beneficial effect for widening communication channels, Data Protection Commissioners continue to address the problem of users' readiness to give away their personal information so readily. Here is a description of the main countries that have responded to SNS (this is not exhaustive). The countries were chosen to illustrate how they have approached social networking issues in a data protection context.

Australia

In Australia, the Privacy Commissioner posted a press release titled 'Protect your privacy on social networking sites, says Privacy Commissioner.'[26] The advice from the Australian Privacy Commissioner to users of social networking websites is simply to be aware of the risks and taking a common sense approach to looking after your personal information, including reading your privacy policy and asking individuals to be careful about what information they give. To date, there have been no legal cases brought in Australia relating to social networking and privacy.

Canada

The Canadian Privacy Commissioner[27] has been proactive in warning of the dangers of using social networking websites and individuals giving away personal information. The Privacy Commissioner has produced a video highlighting the perils of SNS entitled 'What does a friend of a friend of a friend need to know about you?'[28] The latest news was that four students have lodged a complaint before the Privacy Commissioner in Canada claiming that Facebook had given their personal information to marketers without their consent.[29] The Privacy Commissioner has recently decided that Facebook breaches the Canadian PIPEDA Act and has recommended changes.[30] The decision is of significance because the changes will not only apply to Facebook, but impact upon other social network providers in Canada.[31]

Germany

Before one discusses the current developments in Germany, a brief description of the German Data Protection Framework.[32] The German Federal Data Protection Act 2001 applies to federal public bodies and private organisations. The State ('Land') data protection laws applies to state public bodies. As for online activities, this is covered under the German Telemedia Act, which replaces the German Teleservices Data Protection Act 1997 and German Teleservices Act 1997.

On the question of the application of the German Telemedia Act to social networking sites, unless the profile is private, then it would fall within the scope of the Act. What is unclear is whether the Federal Data Protection Act 2001 would cover individuals who post information about other individuals that may have an adverse effect and whether this would be exempted for the purposes of "literary or journalistic purposes". Following queries with the Berlin Data Protection Commissioner, the main response is as follows:

> *'…Third party personal data contained e.g. in a social network subscribers' profile. Whether a subscriber would be held as a controller of such data, will depend on the degree to which these data are accessible to others. E.g. a photo album held on the server of a social network provider only accessible to the subscriber himself would fall under the exemption for "purely personal or household activities" in Art 3 para 2 of Directive 95/46 resp Para 1 section 2 No 3 of the Federal German Data Protection Act. If such data are made available to others, the subscriber may well be held as a* controller of such data depending on the degree of public availability. This would need to be determined according to the circumstances in every single case' *(emphasis added).*

The Berlin Data Protection Commissioner has since, published guidelines on social networking and data protection issues.[33] Through translation of the guidelines, online providers should ensure that that they are fully compliant with the processing of personal data and their choice and design options. The use of personal data online for advertising purposes must also accord with the Telemedia Act (*Telemediengesetz)*, which came into force on March 2007.

According to one legal expert on data protection issues in Germany, someone who uploads the material to a social networking site would be regarded as the controller of the data until it is uploaded.

> *'The social networking website would become the data controller. Even if these social networking websites were to use the exemptions on grounds of press privileges, this would not exclude the application of the Federal Data Protection Act or the Teleservices (sic: Telemedia) Act. Content is generally dealt within the Teleservices (sic: Telemedia Act). The Act also complies with the E-Commerce Directive and would be interpreted in the light of the Directive.'*

Some examples involving social networking included the German Student Community Studi VZ (ca 10 Mio user), which changed their terms and conditions in January to enable them to monitor traffic in order to generate information for advertisement and to pass information to Law enforcement (without legal obligation to do so, using an implicit 'consent'). While there was enormous protest, very few people left StudiVZ.[34]

To date, there have been no actual legal cases determining the extent of the application of data protection laws to social networking in Germany. It is likely that the Federal Data Protection Commissioner's guidelines will align their view to the recent Article 29 Data Protection Working Party's opinion on social networking.

Sweden

The Personal Data Act 1998 regulates the processing of personal data in Sweden and implements the Data Protection Directive 95/46/EC.[35]

There have been guidelines issued by the Swedish Data Inspection Board ('DIB') on social networking. On a specific point relating to the scope of 'data controller' within the definition of the Data Protection Directive 95/46/EC, this question is still to be determined by the DIB. The DIB has not yet had any specific cases regarding websites nor issued any formal opinions on this subject. According to the DIB, the Personal Data Act 1998 is applicable to personal data that is published by people or organisations who are

established in Sweden. The only difficulty that may arise is tracing the source of the information (the 'infringer' for posting personal information online).

The DIB has however has issued some results into a study carried out at the beginning of 2008 on young people's views on Facebook.[36] According to the report, half of the young people had been subjected to someone lying or writing unfair things about them on the internet:

> *'One out of five has experienced someone else using their identity, and 29 per cent of the queried girls say they have been subjected to sexual harassment on the Internet. Eighty-six per cent have published photographs of themselves. However, there is a great deal of resistance to others publishing photographs without asking permission, but 30 per cent have been subjected to this.'*[37]

According to the DIB, notwithstanding these offences, young people still expose themselves on the internet that is unthinkable in real life. The DIB has indicated that more needs to be done and this is expressed by Göran Gräslund, Director-General of the DIB:

> *'Behaviour that involves risk does not seem to be attributable to lack of knowledge; rather, the problem seems to be a basic attitude to personal integrity. If we are to change attitudes, everyone must help: decision-makers, teachers and especially parents.'*[38]

United Kingdom

The UK Information Commissioner (ICO) has also been quite active in publishing guidelines on social networking and privacy recommending that youngsters should not put too much personal information on such social networking websites. According to a survey taken by Viadeo, 62 per cent of British employers do check SNS with the result that a quarter of potential candidates are rejected.[39]

According to the latest Ofcom study into the use of social networking sites, the average social networker has profiles on 1.6 sites with the average user checking their profile each day. Some 39 per cent of adults have profiles of two or more sites. The study highlights the distinct groups in which these users fall under:

- **Alpha socialisers (a minority)** – people who used sites in intense short bursts to flirt, meet new people, and be entertained.
- **Attention seekers** – (some) people who craved attention and comments from others, often by posting photos and customising their profiles.
- **Followers** – (many) people who joined sites to keep up with what their peers were doing.
- **Faithfuls** – (many) people who typically used social networking sites to rekindle old friendships, often from school or university.
- **Functionals** – (a minority) people who tended to be single-minded in using sites for a particular purpose.[40]

In recent correspondence with the UK Information Commissioner it was revealed that since 2005 two complaints have been received about Bebo, one in 2007 and one in 2008. Five complaints were lodged against Facebook, and no complaints were received about MySpace. According to the the ICO:

> *'One of the enquiries we have received about Bebo was from an individual who stated that an account had been opened in his son's name. Bebo had subsequently cancelled the account, but the enquirer was concerned that personal data relating to the account may have been retained by Bebo. He was advised his son could consider issuing a notice under section 10 of the Data Protection Act 1998 against Bebo…The complaint about Facebook also concerned an account which had been opened in the complainant's name. The complainant had notified Facebook of this, and Facebook had closed the account. However, Facebook subsequently refused to tell the complainant when the account was created, how many users had accessed it, or to contact users to tell them that the account had been closed down because it had been created without the complainant's knowledge or consent.*
>
> *'We notified the complainant that no action could be taken because Facebook is not a UK based company. Also, that even if this was not the case, the complainant had not right of access to any information concerning the account because it was opened by someone else, and so the information was not the complainant's personal data. The complainant was advised that if he suspected fraud or harassment he should contact the local police.'*[41]

Whilst the correspondence was fairly recent, it does not take account of the cases alluded to earlier. The significant case of *Applause* is likely to bring into sharp focus the extent to which users can bring legal action against others under the Data Protection Act even if this is on privacy grounds.

International Working Group on Data Protection in Telecommunications

The International Working Group on Data Protection in Telecommunications (hereinafter the 'working group') published guidelines into the use of SNS and privacy in March 2008, which require some perceptive analysis before concluding this section.

It took the view that legislators, data protection authorities and social network providers were faced with a situation that had no visible past. The working group recognised that once personal information was published on the internet, it may stay there forever even when the data subject has deleted it from the original site. The working Group also identified that there was a misleading notion of '*community*' in a SNS which would lead individuals to readily share personal information and that platforms (such as MySpace) created the illusion of intimacy on the web. Traffic data was frequently collected by social network providers. There was potential misuse of profile data by third parties, which also depended on the privacy settings that were available. The working party also found that one third of human resources managers admitted to using data from social networking services. The working group was particularly concerned about the rise in identity theft through the proliferation of user profiles.

The main recommendations worth noting are that the working party took the view that service providers should be honest and clear about what information was required so that users could make informed choices whether to take up the service. It also recommended the introduction of data breach notifications by service providers, so that users could be informed and make choices. One of the most significant recommendations is that the current regulatory framework be reviewed with respect to controllership of 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 networking providers. It concluded by indicating that the working party will closely monitor future developments and revise and update the guidance where necessary.

Article 29 Data Protection Working Party's opinion on social networking

The recent Article 29 Data Protection Working Party's opinion on social networking is likely to be of significance since it has clarified the extent to which users may or may not be considered as 'data controllers.' It took the view that in general users would be subject to the article 3.2 category, processing for private purposes ('household exemption'). However, users may still be regarded as 'data controllers' if their activities go beyond the private purposes category, such as acting on behalf of a company or association, or using the social networking site to promote charitable or political aims. Whilst the opinion concentrated mainly on the application of private purposes, it would also have been useful to clarify the extent to which other exemptions such as article 9 ('artistic, literary and journalistic') may apply. A hypothetical practical example where this may occur is where X is a journalist, but has a blog, Facebook profile, and an organisation profile. Under those circumstances, it is very unlikely that X's profile would fall within the article 3.2 category unless he was not acting in his capacity as a journalist. The journalistic provisions may be applicable, but even then it would be difficult to ascertain whether X was using the social network as a 'journalist' or rather in his private capacity. This would be further extended towards other professions such as accountants, lawyers and teachers. Again, it would be more advantageous for article 3.2 to be applied, which would require a clear disassociation from their professions.

The Article 29 Data Protection Working Party also took the view that social network providers and, in some circumstances, application providers, would be considered as 'data controllers' within the Data Protection Directive. Information about third parties (such as adding a name to a picture etc) would have to operate under article 7 of the Data Protection Directive, which raises issues of required consent by the data subject, contractual obligation and so forth. Again, compliance with these principles may be difficult in the context of social networking. However, if one considers the Facebook environment, there is a mechanism for members to alert Facebook if other Facebook users are not operating within the terms of agreement, which is a starting point.

In short, the Article 29 Data Protection Working Party's opinion is to be welcomed for clarification on the extent of Data Protection Directive 95/46/EC to social network providers and users.

Consequences of Web 2.0 Technologies within SNS

The next question deals with the negative connotations of using SNS and the *consequences* of the loss of privacy of personal information within a social networking context. To give a hypothetical example, if I create a profile, am I responsible for what someone else puts on my profile page? The Article 29 Data Protection Working Party's opinion has indicated that in some instances individuals may assume 'data controller' responsibilities. The difficulty lies with the attribution of responsibility on individuals, in that the less observant individual is unlikely to regularly check their SNS profiles, yet third parties such as prospective employers, journalists and even educational establishments (as shown in the case of the Oxford student scenario)[42] are more likely to use SNS and thus, form their impression (positive or negative) of the individuals. Other than the loss of productivity in workers for using SNS such as Facebook, a potential consequence is liability for a defamatory post (under defamation laws) and possibly misuse of personal information (*applause*), lending itself to further queries by some commentators whether SNS is likely to lead to a rise in caselaw. If SNS is misused, then the law may intervene to rectify a false profile or defamatory statement posted online, precisely because SNS had simply 'got out of line.'

These potential *negativities* arising from the *misuse* of SNS and can be summarised as follows (not exhaustive):

- potential *liability* arising under a defamatory claim from third parties;
- loss of *potential job/existing job* based on individual's SNS profile – inferences drawn by prospective/existing employers on the prospective/existing employee's SNS profile;[43]
- loss of *reputation* based on SNS profile;
- loss of identity through 'identity theft';
- merger of boundaries between an individual's *personal* and *professional* life through the use of SNS;
- individual profile created on SNS can still be searchable on search engines;
- virtual identity created online would be difficult to delete even with sophisticated technologies;
- possibility of linkage between SNS profile to other websites and users' clickstream data, thus creating a virtual profile;
- criminal offences that may occur through the misuse of individual's personal information, such as cyber-stalking and harassment.[44]

The above examples illustrate some of the problems arising under a SNS, but it should not be forgotten that one is dealing with negativities rather than the positive effects of SNS. The key is that if individuals are likely to be attributed responsibility for the information they post on their profile, are they likely to be more careful with what they put on this profile? Other than using existing controls to limit the amount of personal information, are they likely to be proactive in the way they give their personal information including their hobbies, habits, pastimes and so forth? Sounding alarm bells on the potential negativities may be one possibility,[45] but emphasising the relative ease in which individual's profile can be easily accessible to identity thieves and unwanted third parties is also another way to alert individuals to being more cautious.

You can't be too careful with your personal information: privacy conscious or privacy smart?

With enough publicity by newspapers of security breaches of personal information and numerous guidelines on SNS produced, is it not possible to underestimate the ways in which individuals protect their personal information? To put it another way, is it possible that some individuals can become privacy conscious or privacy smart? With enough technological controls in limiting the amount of personal information, surely, this should be possible. According to one report[46] in Canada, more than half of Canadians would be concerned about giving their personal information to their retailers. The question is, why not apply this to a social networking setting? In other words, educate users to become more 'privacy savvy' so that more people do not give their personal information away so easily.

Indeed, one retired lawyer remarked on the rise of blogs and social networking sites, 'why would you want to write anything

about your personal life on these blogs?' and 'who reads these things?' Whilst he comes from a generation where computers did not become mainstream, yet his view highlights a clear division in opinion over the value of blogs.

According to the latest OFCOM study,[47] it was found that social networking sites were most popular with teenagers and young adults and that two-thirds of parents claim to set rules on their child's use of social networking sites, although only 53 per cent of children said that their parents set such rules.

Conclusions

To conclude, social networking websites are perceived to be a harmless activity, particularly amongst friends and colleagues including causes that they may share, yet the article highlights a difficulty with the current legal data protection framework as an attempt in applying the old law to new uses. The Article 29 Data Protection Working Party's opinion seeks to clarify the extent to which users are regarded as 'data controllers' within an SNS, particularly in the context of third party applications (presumably the ultimate decision is for the ECJ as article 29 reports are opinions and not binding). Some SNS have already started to indicate that users are 'data controllers' of the profiles they put on their website. It is acknowledged that social networking can be accessible by third parties, yet the data protection principles clearly state that the user's right to give information out for one purpose is not to be used for another purpose. On a practical level, it would be fairly difficult to see how this principle can be achieved. Although the prospect of bringing lawsuits within a social networking website is unlikely to be attractive to many, for the few who do decide to take this up the question is whether this is the appropriate method in protecting one's identity or reputation.

The data protection authorities have started to look into this subject,[48] but other than educating the younger adults about the wider availability of their personal information beyond their inner circle of friends, there is also the issue of understanding the limitations in the enforcement of the data protection framework. Again, the impetus would be upon individuals to take proactive action to protect their identity. Revising the private exemption in article 3.2 to exclude private users for non-commercial purposes from the definition of data controllers is one objective which would have to be achieved at European level. Facebook should also consider introducing take-down procedures for third parties who wish to remove material from a profile because there has been a misuse of their personal information. A final concluding remark is that the national data protection authorities should ensure that the rigours of the national Data Protection Acts are applied sensibly to social networking sites and that only those who are culpably blameworthy for the use and misuse of an individuals' profile are held accountable. As one learned piece of advice goes: 'Common sense is the best I know of' (per Lord Chesterfield).

Dr Rebecca Wong

The author is Senior Lecturer in Law at Nottingham Law School, Nottingham Trent University with teaching and research interests in tort, intellectual property, data protection and cyber law. Her main areas of specialism are in data protection and privacy. She recently guest edited a special issue on 'Identity, privacy and new technologies' in the *International Journal of Intellectual Property Management* 2008/9. She can be reached at R.Wong@ntu.ac.uk

The author would like to thank the following for their helpful assistance during the writing of this article: Dr Mark Taylor, University of Sheffield; Dr K Chamundeeswari, University of Sheffield; Berlin Data Protection Commission; Elisabeth Wallin, Swedish Data Inspection Board; Mr Sören Őman, Ministry of Justice, Sweden; Dr Thomas Probst, Schleswig-Holstein Data Protection Commissioner's Office; Dr Ulrich Wuermeling, Latham and Watkins, UK Information Commissioner's Office. Views expressed are entirely those of the author. CL

Notes

1 Quotation from the article in Kim Hart, 'A flashy facebook page, at a cost to privacy, *Washington Post,* available at http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html, 12 June 2008.

2 The author is not concerned with the technological measures that are available on Facebook, MySpace which can restrict access of users' profile to certain categories of individuals. This issue has addressed in a recent article, Gray, T T Zeggane, & W Maxwell, 'US and EU authorities review privacy threats on social networking sites' (2008) *Entertainment Law Review* 69.

3 In this article, reference is made to user-generated content with users uploading their personal profiles on Flickr, Facebook, MySpace and Bebo.

4 Cf. Consider also the Canadian view on their legal framework to protecting individuals available at (http://www.pitblado.com/lawyer_images/Lawyers_Weekly_-_jTechnology_drives_need_for_new_privacy_legislation.pd), which raises the discussion over third generation privacy laws. Looking at the current statistics from the Facebook website, there were more than 130 million active users with the average user having 100 friends on the site (available at http://www.facebook.com/press/info.php?statistics).

5 Verkaik, R, 'New front in the battle against identity theft' *The Independent*, November 23, 2007.

6 Boyes, R, 'And this is me on Facebook…helping with brainysurgery' *The Times,* August 18, 2008.

7 On a broader question on the application of art 3.2 Data Protection Directive to the internet, see also Wong, R, and Savirimuthu, J, 'All or nothing, this is the question: the application of art 3.2 Data Protection Directive 95/46/EC to the internet', *John Marshall Journal of Computer and Information Law*, 2008, 25, 241.

8 [2008] EWHC 1781.

9 For a detailed analysis of the tortious right to misuse of personal information, see *Campbell v MGN* [2004] UKHL 22 and Fenwick, H and Philippson, G, *Media freedom under the Human Rights Act* (Oxford University Press, 2006), pp 728-70.

10 *Applause Store Productions Ltd and Anor v Raphael*, *op cit n 8,* at para 80.

11 At the time of writing this article, the 30th International Data Protection Commissioners' Conference was held in Strasbourg, with a symposium to consider the issues arising from social networking sites. This is available at http://www.datenschutz-berlin.de/content/Berlin/Berliner+Beauftragter/Veranstaltungen/Symposium+2008

12 See the Article 29 Data Protection Working Party, opinion 5/2009 on Social Networking available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf, dated June 12, 2009.

13 See Article 29 Data Protection Working Party, opinion 5/2009 on online social networking available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf, and *Daily Telegraph*, 'Social networking sites could be embroiled in privacy crackdown' at http://www.telegraph.co.uk/scienceandtechnology/technology/technologynews/5570008/Social-networking-sites-could-be-embroiled-in-privacy-crackdown.html, dated June 18, 2009.

14 See also Edwards, L and I. Brown, 'Data control and social networking: irreconcilable ideas', in A Matwyshyn (ed, *Harboring data: Information security, law and the corporation*, 2009.

15 C-73/07, OJC44 of February 21, 2009 at p 6. The case concerned the collation and publication of publicly available details of Finnish taxpayers which were initially published in regional newspapers and were then forwarded to a sister company of the newspaper publisher on CD-Roms with a view to the information being made accessible via a text messaging service – paras 52-62 relate to the journalistic exception. The exception applies to all journalistic activity (para 58) and can be to make a profit, in this particular case from people paying to

receive text messages, and can be within the exception 'if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes' (at para 61) – possibly amateur 'journalists' on Facebook?

16 [2002] EWCA Civ 1373.

17 See also White, Anthony, 'Data protection and the media', *European Human Rights Law Review* (2003) 25-36.

18 Full title of the Data Protection Directive 95/46/EC is 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, *Official Journal L 281 , 23/11/1995 P 0031 – 0050.*

19 [2004] QB 1041.

20 The UK Data Protection Act 1998, however includes 'recreation' within s 36 of the DPA 1998 and it is arguable that profiles created would fall within this notwithstanding the difference from the European Data Protection Directive 95/46/EC.

21 To date, Argentina, Hungary, Switzerland, Canada (whereby its Personal Information Protection and Electronic Documents Act applies), Guernsey and the Isle of Man are considered to be adequate under art 25 Data Protection Directive by the European Commission. The US has an agreement with the European Union known as the safe harbour principles in which companies self-certify to a set of principles akin to those of the DPD.

22 On the subject of sensitive personal data, see Simitis, S *Revisiting sensitive data* (http://www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/Documents/Reports/W-Report%20Simitis.asp#TopOfPage), 1999 and Wong, R 'Data protection online: Alternative approaches to sensitive data', *Journal of International Commercial Law and Technology* (2007) 2(1) 9-16.

23 Cf McGarr, S, 'Facebook's compliance with European data protection law', *Data Protection Law and Policy*, March 2008, 8-9.

24 Available at http://www.myspace.com/index.cfm?fuseaction=misc.privacy

25 One example would be if individual A had mentioned individual X (whether by name or indirectly) on a social networking profile in order to highlight certain offences committed by individual X, and from this information it was readily identified that this referred to X. If there is some validity in the claim, then art 13(1)(g) may be used by individual A to contend that the Data Protection Directive would not apply as X's actions were to protect others.

26 Available at http://www.privacy.gov.au/news/media/2007_23.html

27 Available at http://blog.privcom.gc.ca/index.php/2007/10/10/social-networking-and-privacy/

28 Available at http://blog.privcom.gc.ca/index.php/privacy-on-social-networks/

29 *Canada's Privacy Commissioner launches Facebook probe after law students file complaint* available at http://www.iht.com/articles/ap/2008/05/31/business/NA-GEN-Canada-Facebook-Probe.php, dated May 31, 2008. *Canadian Group files Facebook Privacy Complaint* available at http://tech.slashdot.org/article.pl?sid=08/06/02/0010220, Dated June 2, 2008.

30 See Privacy Commissioner. *Report of findings into the complaint filed by the CIPPIC against Facebook Inc under PIPEDA* at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm.

31 Canadian Commission concludes Facebook is too snoopy, *E-Commerce Times* at http://www.ecommercetimes.com/story/67611.html dated July 16, 2009.

32 For a commentary on German Data Protection Laws, see Simitis, S *Kommentar zum Bundesdatenschutzgesetz*, Baden-Baden: Nomos, 2003.

33 *The Common position of of German Data Protection Oversight Authorities for the private sector ('Düsseldorfer Kreis') of April 2008*, http://www.datenschutz-berlin.de/attachments/487/D__sseldorfer_Kreis_April_2008_Datenschutzkonforme_Gestaltung_sozialer_Netzwerke.pdf?1212737975 (in German only).

34 For more on this, see *Internet 2008 - Alles möglich, nichts privat?* available at https://ntuanywhere.ntu.ac.uk/sommerakademie/2008/,DanaInfo=.awxyChfzlv1ms66BCu4.-C7V02,SSL+

35 For a detailed commentary into Swedish developments on data protection, see Blume, P (ed), *Nordic Data Protection Law*, (Copenhagen: DJOP, 2001) as a starting point.

36 The study is available in Swedish only and can be found at http://www.datainspektionen.se/Documents/rapport-ungdom2008.pdf

37 Data Inspection Board. *Every other young person has been offended on the internet* available at http://www.datainspektionen.se/in-english/every-other-young-person-has-been-offended-on-the-internet/

38 *Id.*

39 Bergstrom I, 'Facebook can ruin your life. And so can MySpace, Bebo…', *The Independent* available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html

40 Ofcom. *Engaging with social networking sites available* at: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

41 Written correspondence from the ICO dated September 30, 2008.

42 BBC. *Unruly students' facebook search* available at http://news.bbc.co.uk/1/hi/education/6902333.stm, July 17, 2007.

43 This can be likened to the right to silence where this issue is not the defendant's right not to speak, but also adverse inferences should not be drawn by the prosecution for the defendant's right not to speak. Indeed, it was shown that 62 per cent of British employers now check Facebook, MySpace and Bebo (see also Bergstrom, I, 'Facebook can ruin your life. And so can MySpace, Bebo..' *The Independent*, February 10, 2008 available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html and Mann, B.L. "Social networking websites – a concatenation of impersonation, denigration, sexual aggressive solicitaiton, cyber-bullying or happy slapping videos" *International Journal of Law and Information Technology*, 2008, doi:10.1093/ijlit/ean008 available at http://ijlit.oxfordjournals.org/cgi/content/citation/ean008v1.

44 Mann, B L, 'Social networking websites – a concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos', *International Journal of Law and Information Technology* available at http://ijlit.oxfordjournals.org/cgi/content/full/ean008, Last accessed 14 October 2008 and Bergstrom, I, 'Facebook can ruin your life. And so can MySpace, Bebo…', *The Independent* available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html.

45 Mann, B L, *op cit* n 34 – Mann takes the view that scare tactics maybe one option to consider to illustrate the privacy concerns in a social networking website. 'Scare tactics that work for habitual drunk drivers may be needed for habitual SNW users acting actus reus, such as television commercials showing users in jail and others who have lost their job as a result of the UGC they generated in a SNW.'

46 *Canadians concerned about giving retailers their personal information* available at http://www.privcom.gc.ca/media/nr-c/2008/nr-c_080703_e.asp

47 Ofcom, *op cit* n 30.

48 See the 30th International Data Protection Commissioners Conference, *Protecting privacy in a borderless world*, Strasbourg available at http://www.privacyconference2008.org/index.php?page_id=1. Panel sessions were convened to address several issues of privacy including social networking sites.