Social networking: a conceptual analysis of a data controller

Rebecca Wong, Nottingham Trent University
Social Networking:
A Conceptual Analysis of a Data Controller

Dr Rebecca Wong¹

ABSTRACT

This paper will look at the definition of a “data controller” within the Data Protection Directive 95/46/EC and consider whether the phenomenon of social networking (through Facebook (FB), MySpace and Bebo) has produced unintended consequences in the interpretation and application of the Data Protection Directive 95/46/EC to the online environment. The Data Protection Directive 95/46/EC defines a “data controller” broadly to refer to the ‘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.’

If the definition of the Data Protection Directive 95/46/EC (DPD) is applied literally to social networking sites such as Facebook and MySpace, arguably, not only organisations such as FB and MySpace are regarded as “data controllers” (through Art. 4 of the DPD), but individuals who posted information about others (friends or work colleagues etc.) would also be regarded as “data controllers” and thus have to adhere to the legal rules laid down under the Data Protection Directive 95/46/EC (ie. Art. 7 of the DPD fair and lawful processing; not excessive etc) unless it could be shown that the exemptions under Art. 9 that processing was intended for journalistic, artistic and literary purposes or that Art. 13 exceptions apply. As identified in an earlier paper, Art. 3.2 DPD (Wong and Savirimuthu, Art. 3(2) All or Nothing: This is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet) is unlikely to apply whereby processing was carried out for private and domestic purposes. This paper is an attempt to address a definitional difficulty that the legislatures did not anticipate. In attempting to protect the privacy of individuals, it is now possible to argue that it is becoming easier for individuals (and not merely organisations) to be brought

¹ Dr Rebecca Wong 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.
within the scope of the Data Protection Directive 95/46/EC in a social networking environment.

Keywords: Data protection; social networking; privacy; data controller

Contents

Introduction.............................................................................................. 2
Dilemmas ................................................................................................. 3
Who is a “Data Controller”? ................................................................. 6
Data Protection Directive 95/46/EC and its application to SNS .......... 8
Work of the Data Protection Commissioners ................................... 11
Australia ............................................................................................. 11
Canada ................................................................................................. 11
Sweden .................................................................................................. 14
UK ......................................................................................................... 15
International Working Group on Data Protection in Telecommunications................................................................. 16
Consequences of Web 2.0 Technologies within SNS............................ 17
You can’t be too careful with your personal information:
privacy conscious or privacy smart? ..................................................... 19
Conclusions.......................................................................................... 20

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”.

Introduction

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”. If one examines the

---


3 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
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, 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. 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.

**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 review privacy threats on social networking sites” (2008) Entertainment Law Review 69.

---

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

5 Cf. Consider also the Canadian view on their legal framework to protecting individuals available at (http://www.pitblado.com/lawyer_images/Lawyers_Weekly_-_Technology_drives_need_for_new_privacy_legislation.pdf), 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).
activities of organisations in processing personal data, 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 easy 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.6

Similarly, the Watchdog, BBC Consumer Programme had 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 identity of the friends were stolen and details used to open an online bank.7

Whether the application to users of SNS would be strictly enforced by data protection authorities or individuals when something goes


7 Boyes, R. “And this is me on Facebook...helping with brainsurgery” *The Times*, 18 August 2008.
wrong is not yet certain. Broadening the framework to include users would raise the question whether social networking website is likely to be stifled. Another perspective would be that the framework would be to heighten awareness and responsibilities of users in a user-generated environment. Whilst the data protection framework is not entirely satisfactory in adapting to SNS, SNS poses a challenge for Data Protection Authorities to rethink the direction of the data protection framework as applied online.

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* 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 Firsh'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 the tort of misuse of personal information is one 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 s 1 of the Data Protection Act 1998 and may even constitute the processing of “sensitive” personal information within s 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

---

8  [2008] EWHC 1781.

10  *Applause Store Productions Ltd and Anor v Raphael*, op. cit. n. 8, at para. 80.
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”,\footnote{At the time of writing this article, the 30\textsuperscript{th} 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 \url{http://www.datenschutz-berlin.de/content/Berlin/Berliner+Beauftragter/Veranstaltungen/Symposium+2008}.} it does call for a rethink in the approach by legislators, Art. 29 Working Party 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”.\footnote{See the Art. 29 Working Party, Opinion 5/2009 on Social Networking available at \url{http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf}, Dated 12\textsuperscript{th} June 2009.} 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 (\textit{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 Art. 29 Working Party had issued a recent opinion that users would generally be covered under the Art. 3.2 private purposes exception, but could, in limited circumstances had data protection responsibilities, if they fall outside the scope. An example given would be where the SNS was used as a collaboration
platform for a company. 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 is that if individuals are viewed as “data controllers” 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, Art. 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 Art. 9 of the Data Protection Directive. However, in a recent case of Tietosuojavaltuutettu v Satakunnan Markkinapörss Oy, Satamedia Oy, 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. s 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 s 32 cannot entirely apply to social networking websites, it would only do so in the limited circumstances described above. Although the application of s 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 that s 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 s 32(4) and (5) were purely procedural aimed at providing for the stay of proceedings against a publisher until after publication.15

The other exemption that may override the protection of an individual’s personal privacy is Art. 13(1)(g) of the DPD on the protection rights and freedoms of others. To date there have been no legal 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 Arts. 7 and 8
2) Rights of the data subjects under Art. 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 Art. 29 Working Party has indicated recently the application of Art. 3.2 of the Data Protection Directive to a social networking environment, the Lindqvist 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.

The ECJ has interpreted the scope of Art. 8 of the Data Protection Directive 95/46/EC on sensitive data widely and had held that Art. 3.2 would be unable to avail on the basis that information is available/accessible to anyone on the internet (no discussion was made by the ECJ of restricting access using intranets).

Art. 4 of the Data Protection Directive applies to user-generated content based within the EU. Art. 4(1)(a) of the Data Protection Directive

---


17 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.

Directive provides that this Directive (or corresponding national data protection laws implementing the Data Protection Directive) applies to activities of an establishment of the controller on the territory of the Member State and/or Art. 4(1)(c) uses equipment to process. For example, in the example of MySpace, there are potentially two data controllers. Firstly, MySpace that holds the personal information of their users and secondly, 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 s 5(1)(a) of the DPA 1998. A data controller is established in the UK and the data are processed in the context of that establishment. The alternative would be if MySpace uses equipment to process personal data within s 5(1)(b). If s 5(1)(b) applies, then the data controller (MySpace) would be required to nominate a representative within the UK.\(^\text{19}\)

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).\(^\text{20}\)

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.

Art. 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. 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 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**

The question is 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 this takes a limited cautious approach about users posting information rather than recommend 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 continues 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”. 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 of Canada 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 entitled What does a friend of a friend of a friend need to know about you highlighting the perils of

---


23 Available at http://blog.privcom.gc.ca/index.php/privacy-on-social-networks/
SNS. 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. The Privacy Commissioner has recently decided that Facebook breaches the Canadian PIPEDA Act and has recommended changes.

Germany

Before one discusses the current developments in Germany, a brief description of the German Data Protection Framework. 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. Through translation of the guidelines, online providers should ensure 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 & Conditions in January to enable them to monitor the 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.

To date, there has been no actual legal cases determining the extent of the application of data protection laws to social networking in Germany.

---

27 For more on this, see Internet 2008 - Alles möglich, nichts privat? available at https://ntuanywhere.ntu.ac.uk/summerakademie/2008/,DanaInfo=.awxyChfzlVlms66BCu4.-C7V02,SSL+. 
Sweden

The Personal Data Act 1998 regulates the processing of personal data in Sweden and implements the Data Protection Directive 95/46/EC.\(^\text{28}\)

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. Following questions with the Swedish Data Inspection Board, it has not yet had any specific cases regarding websites nor have 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 Swedish Data Inspection Board, however, has issued some results into a study carried out among young people at the beginning of 2008 on young people’s views on Facebook.\(^\text{29}\) 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.\(^\text{30}\)

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,

\(^{28}\) 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.

\(^{29}\) The study is available in Swedish only and can be found at http://www.datainspektionen.se/Documents/rapport-ungdom2008.pdf.

\(^{30}\) 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/.
everyone must help: decision-makers, teachers and especially parents.\textsuperscript{31}

UK

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\% of British employers do check SNS with the result that a quarter of potential candidates are rejected.\textsuperscript{32}

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. 39\% 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.\textsuperscript{33}

In a recent correspondence with the UK Information Commissioner, it was identified that since 2005, they have received two complaints about Bebo, one in 2007 and one in 2008. Five complaints were lodged against Facebook. 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,

\textsuperscript{31} Id.


\textsuperscript{33} Ofcom. Engaging with social networking sites available at: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/.
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.34

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 “Working Party”) has recently
published guidelines into the use of SNS and privacy in March 2008,
which requires 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, they may *stay there
forever* even when the data subject has deleted them 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

34 Written correspondence from the ICO dated 30 September 2008.
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 is 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.

Consequences of Web 2.0 Technologies within SNS

The question that then arises is what are the consequences 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 difficulty lies with the attribution of responsibility on individuals, is 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) 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 “got out of line”.

These are the 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

• Loss of reputation based on SNS profile

• Merge 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 linkability between SNS profile to other websites and such as users’ clickstream data and thus create a virtual profile

• Likely criminal offences that may occur through the misuse of individual’s personal information such as cyber-stalking; harassment

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

36 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% 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, 10 February 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 solicitation, 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.

alarm bells on the potential negativities maybe one possibility,\textsuperscript{38} 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.

\textbf{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 \textit{privacy conscious} or \textit{privacy smart}? With enough technological controls in limiting the amount of personal information, surely, this should be possible. According to one report\textsuperscript{39} 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 saavy” so that idea that “we do not wish to give our personal information” so easily becomes more mainstream.

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?”; “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,\textsuperscript{40} 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\% of children said that their parents set such rules.

\textsuperscript{38} Mann, B. L., \textit{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.”

\textsuperscript{39} Canadians concerned about giving retailers their personal information available at \url{http://www.privcom.gc.ca/media/nr-c/2008/nr- c_080703_e.asp}

\textsuperscript{40} Ofcom, \textit{op. cit.} n. 30.
Conclusions

To conclude, social networking websites are perceived to be 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 Art. 29 Working Party’s opinion clarifies the extent to which users are regarded as “data controllers” within a SNS, particularly in the context of third party applications. Some SNS have already started to indicate that users are “data controllers” of the profiles they put on their website. Whilst 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 potential for lawsuits within a social networking website is unlikely to be desirable, 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, but other than educating the younger adults about the wider availability of their personal information beyond their inner circle of friends, it is also 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. The 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 advice goes, “Common sense is the best I know of.” (per Lord Chesterfield).

Acknowledgments

The author would like to thank the following for their helpful assistance during the write up 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 Öman, 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 of the author’s.

41 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.