Impersonation of Life
"The Perils of Social Networking"

Daniel B. Garrie, Esq.[1]
The Honorable Maureen Duffy-Lewis[2]
Rebecca Wong, Esq.[3]
Mari Joller
Richard L. Gillespie, Editor[4]

Users of social networking sites ("SNS") and platforms are realizing their personal information, given for what was believed to be for "limited purpose", has been hijacked, sold, repackaged, misused, abused and otherwise laid bare to the world.

As the user realizes their dilemma, their brow becomes furrowed and drips with sweat caused by frustration and concern. While they wring their hands with despair, they ask themselves, "How could this have happened?", "Who do these people think they are?" and in the worst case scenario, identity theft, "Who is this person and why is he 'ruining my life?'"

This article examines how information from social networking sites can be intentionally or unwittingly transferred and the many consequences, which could then flow to users, vendors and back to the SNS. Laws governing data protection vary from country to country. Developing new or updated legal protocols leave those charged with the development in a race against technology, a race which technology seems to always have a "head start" in. The European Union and the International Working Group

[1] **Daniel B. Garrie, Esq.**, is Managing Director at the venture capital firm EMI Capital LLC (www.emicapital.com) and a court-appointed e-discovery neutral via Alternative Resolution Centers (ARC). Prior to joining ARC, Mr. Garrie was the Director of e-discovery at CRA International (a global consulting firm that provides economic, financial, strategy, and business management advice to law firms, corporations, accounting firms, and governmental organizations). Mr. Garrie lives in New York and can be reached at dgarrie@emicapital.com. He would also like to thank both Chirag Patel and Mari Joller for their help with the article.

[2] **The Honorable Maureen Duffy-Lewis**, is a Judge of the Los Angeles Superior Court, State of California, United States of America. She currently presides in Department 38 of the Stanley Mosk Civil Courthouse. She may be reached at MDLewis@LASuperiorCourt.org.

[3] **Dr. Rebecca Wong, Esq.,** is a Senior Lecturer in Law at Nottingham Law School Burton Street Nottingham NG1 4BU UK and may be reached at R.Wong@ntu.ac.uk.

[4] **Richard L. Gillespie**, Editor, is a second year law student, Pepperdine University School of Law, with assistance and thanks to Andrew Maiorano, also a second year law student at Pepperdine University School of Law.

on Data Protection are forging ahead with recommendations, laws and guidelines, but seem to be playing "catch-up" as they attempt to "close the barn door after the horse got out". But could that have been any different, since laws seem to always lag behind human creativity?

Applicable laws such as the Data Protection Directive 95/46/EC ("DPD") address how both social network companies and the individual can be classified as "data controllers".[5] The DPD states that a data controller:

> 'Shall mean 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.'[6]

The language defining "data controller" seems to support the view that individuals who post information about others on the internet would be regarded as "data controllers". Since social networks and their users, assume the roles of "data subjects" and "data controllers", through the publishing of oral and/or written information about others, by friends, colleagues and associates,[7] then it follows that the DPD would apply. However, would the DPD apply to social networking technologies? For example, who are our users/data subjects? What are the obligations for data controllers under the data protection laws? How easily would information (and potentially false information) be circulated about others and would there be the opportunity to remedy the damage? And if such an opportunity exists, then how far and to whom should liability extend?

---

[5] *See* Council Directive 95/46, art. 2(d) 1995 O.J. (EC).
[6] *Id*.
[7] This is not to indicate that it is likely to lead to more legal action, but it is questionable whether this is an appropriate forum for deciding privacy cases.

As technology races forward, it is leaving its corresponding legislation "in the dust". The current liability for user-generated content under the DPD and the application of the DPD to the SNS is sorely inadequate, and it is our view that the European Union must re-evaluate the direction of the data protection framework as applied online,[8] to better protect individuals and to prevent the rise of litigation disputes from flooding the courts.

Whether the application to users would be strictly enforced by Data Protection Authorities or by individuals, when complications arise is not yet certain. Broadening the framework to users would raise the questions whether social networking websites are likely to be stifled or if it would simply heighten the awareness of the responsibilities of users in the user-generated environment.

There have been few cases dealing with user generated content and liability under the DPD 95/46/EC. One significant case that arose before the courts in the United Kingdom is *Applause Store Productions, Ltd.* and *Anor v. Raphael.*[9] This case concerned a user who brought legal action against a former friend who posted a false profile on Facebook.[10] The Court found for the claimant and held on the grounds of "misuse of private information."[11] Under the DPD, since there was no question that some of the statements posted in the Facebook profile were defamatory and sensitive personal information,[12] the Court should hold the individual and the social network responsible.

Today social networks are deploying sophisticated technological measures[13] for the user to protect their privacy settings,[14]but they do not address etiquette.

---

[8] The International Data Protection Commissioners convened a panel to discuss the implications of social networking in October, Strasbourg, 2008, with a resolution published. The panel's recommendations are a*vailable at* http://www.bfdi.bund.de/cln027/nn72110/SharedDocs/Publikationen/EN/InternationalDS/2008SocialNetwork.html (the main recommendations include more user control of profile data; data security; deletion of user profiles; the possibility of providers to enable the creation and use of pseudonymous profiles as an option; The ability to index user profiles to be only permitted on search engines with explicit and prior-informed consent).

[9] [2008] EWHC 1781 (QB).

[10] *Id*.

[11] *Id*., at ¶ 80.

[12] This assumes that this type of posting constitutes the processing of personal data within the DPD.

[13] *See* EDWARDS, L. C. MARSDEN & I. BROWN, CYBERSTALKING 2l0 *available at* http://www.law.ed.ac.uk/ahrc/gikii/papers07.asp.

Unfortunately, the simple solution of removal or deletion of the contentious content, opens other issues[15] as to whether social networks in this context are operating as censors. A proactive step could be to implicate a simple education on user etiquette and the attendant peer pressure,[16] with a limited reactive deletion strategy. These steps would partially remedy a substantial component of the problem, but for now, nothing offers a complete "fix"!

In an effort to understand how the DPD 95/46/EC is applied to SNS, we explored the implications of the application's main provisions, and specifically

- Data protection rights and obligations as laid down under Articles 7 and 8.
- Rights of data subjects under Article 10.
- Data Protection principles as laid down under Article 7 of the DPD.

Any one of these three provisions applied in this context would lead to major questions about the relevance of the framework to the social networking environment.[17] Further complicating matters is the ambiguity as to whether the Directive (or national data protection laws) would be enforced in the strict sense, as personal information is readily available on SNS and that users have consented to have this information accessible to others.[18]

The Directive clearly explains obligations that "data controllers" would need to fulfil, yet in a SNS environment it would be difficult to see how this framework can be accomplished. For example, the first data protection principle requires that data must be processed *lawfully* and *fairly*. To require every user (as a "data controller") within a SNS to do this would be an unrealistic objective, and would also be very difficult for the Data Protection Authorities to police and monitor. Similarly, information provided to data subjects under Article 10 would be easy to request from an organization, but individuals requesting the same information from other individuals within a SNS would

---

[14] *Id*.
[15] *See* J. Grimmelmann, *Facebook and the social dynamics of privacy* (NYLS Legal Studies Research Paper No. 08/09-7 2009)
[16] *See* ICO guidelines on social networking; *see also* Canada's Privacy Commissioner's Guidelines on social networking site.
[17] *See* Grimmelmann, *supra* at note 12.
[18] The DPD requires "unambiguous" consent for the processing of normal data per Article 7(a) of the DPD and "explicit consent" under Article 8 of the DPD for the processing of special categories of data.

be much more difficult to accomplish, and likely be regarded as a futile exercise. Furthermore, it could be argued that Article 10 would be redundant in a SNS, since a profile only contains brief information about users, but not necessarily views or opinions. Another example is that the data protection principle requires that information contained about data subjects be "adequate", not "excessive".[19] Again, this principle is more applicable to an organization. It would be unusual to require a SNS provider to indicate whether a user has necessarily provided "adequate" information about users, since the users themselves are providing the information and are the "data controllers", determining the scope of their profile and what it contains.

Another consideration is the *consent* requirements within the DPD, which will likely not be fulfilled. This requirement will likely not be satisfied because the user will likely only have consented for one purpose,[20] namely, to have their profile available to a limited group, but not necessarily to third parties such as employers or the wider public. Furthermore, privacy terms on a social networking website are viewed as overly unwieldly, and often opaque over the extent to which users have control over their personal profile on a social networking site. However, Facebook's recent change in the terms and conditions resulted in users' protesting over the extent to which they have control. Whilst Facebook has reverted to its original privacy terms, it highlights the unease from users over the leeway that social networking sites have towards their profile.[21] This has been the subject of much discussion and therefore will not be considered here.[22] Finally, the Data Protection Authorities should take a proactive approach to raise awareness on the relevance of the Data Protection laws to social networking sites.[23]

---

[19] *See* Council Directive 95/46 at art. 10.

[20] For an in-depth discussion into SNS, see also Grimmelmann, *supra* at note 12.

[21] *See* BBC. *Facebook says yes to changes* available at http://news.bbc.co.uk/1/hi/technology/8016532.stm, Dated 24 April 2009; Ward, M. *Whose data is it anyway?* Dated 24 April 2009, available at http://news.bbc.co.uk/1/hi/technology/7899456.stm and Open Rights Group. *Facebook theatrical rights and wrongs available* at http://www.openrightsgroup.org/2009/04/01/facebook%E2%80%99s-theatrical-rights-and-wrongs/ and commentary by Michael Zimmer on Facebook at http://michaelzimmer.org/category/facebook/.

[22] *Id.*

[23] Discussions have started with the International Data Protection Commissioners' Conference that was held in Strasbourg (http://www.privacyconference2008.org/index.php).

SNS create difficulties and challenges for the Directive, and imposes responsibilities on individuals (not only organizations) regarding how they use information about others. Whether the legal framework is a suitable forum for resolving civil disputes involving the post/publication of profiles is even less clear.

In a social networking environment, *Article 3.2 of the Data Protection Directive 95/46/EC*[24] is unlikely to assist individuals who wish to benefit from the "private purposes" exemption for posting personal information about others within the online environment.[25] The European Court of Justice's decision in the criminal proceeding, against Bodil Lindqvist[26], liberally interpreted the scope of Article 8 of the Data Protection Directive 95/46/EC on sensitive data,[27] and had held that Article 3.2 would be insufficient on the basis that information is available or accessible to anyone on the internet (no discussion was made by the ECJ of restricting access using intranets).[28] However, even with this interpretation a major problem persists because individuals most certainly will argue that certain sections they post on the internet should be regarded as "private".[29]

The scope of Article 4 of the Data Protection Directive applies to user-generated content.[30] 4(1)(a) of the Data Protection Directive provides that the Directive (or corresponding national data protection laws implementing the Data Protection Directive) applies to activities of an establishment of the controller which are on the territory of the Member State.[31] 4(1)(c) expands this jurisdiction to include areas where equipment is used to process such information (more difficult to show that the user-

---

[24] *See* Council Directive 95/46 at art. 3.2.
[25] Leaving aside the UK Data Protection Act 1998, whereby the wording under section 36 of the DPA 1998 (private purposes) includes "recreation" and would enable the possibility of private web-pages to be brought within this scope.
[26] ECJ Case C-101/01, 1995 O.J. (L 281) 31 (EC) (discussing the interpretation of 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)
[27] *See id*.; *see also* Council Directive 95/46 at art. 8.
[28] REBECCA. WONG & JOSEPH SAVIRIMUTHU, *All or nothing: the application of Article 3.2 of the Data Protection Directive 95/46/EC to the internet*, J. MARSHALL L.REV. 25 (2008).
[29] *See* P. Seipel *Sweden in Nordic Data Protection Law* (P. Blume ed., 2001).
[30] *See* Council Directive 95/46 at art. 4.
[31] *Id*.

generated content falls outside the EEA).[32] For example, MySpace is based in California, U.S.A. There is an arguable case that even if Article 4(1)(a) is not applicable, 4(1)(c) whereby the data controller (MySpace) uses and processes personal data (equipment) may apply. It is possible that internet servers or data protection controllers may relocate in order that their activities may fall outside the jurisdiction of the Data Protection Directive 95/46/EC: Article 4 of the Data Protection Directive 95/46/EC depends on where the data controller is based. It is established that MySpace has an office in the UK (clear that they would be data controllers within 5(1)(a) of the DPA 1998). A data controller is established in the United Kingdom when data is processed in the context of that establishment or uses equipment in the United Kingdom.[33] This corresponds with Article 4 of the Data Protection Directive 95/46/EC.[34]

It should be noted that, *Article 13* of the Data Protection Directive *95/46/EC* limits the scope of the obligations and rights provided for in Articles 6(1),[35] 10,[36] 11(1),[37] 12[38] and 21[39] 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 economics; and (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 there have been no cases to clarify the scope of this final exemption.

Article 9 of the Data Protection Directive provides for exemptions in processing of personal data on the basis of "artistic, literary and journalistic" purposes.[40] It is

---

[32] *Id*.
[33] s 5(1)(b) UK Data Protection Act 1998.
[34] *Id*.
[35] *See* Council Directive 95/46 at art. 6.1 (enumerating the data protection principles).
[36] *See* Council Directive 95/46 at art. 10 (listing the information to be given to the data subject).
[37] *See* Council Directive 95/46 at art. 11 (listing the information to be given to the data subject).
[38] *See* Council Directive 95/46 at art. 12 (providing for the data subject's right of access to their data).
[39] *See* Council Directive 95/46 at art. 15 (providing for the circumstances whereby individual's personal data are subjected to automated individual decision).
[40] *See* Council Directive 95/46 at art 9.

questionable whether SNS, *per se,* would necessarily fulfill the criteria of "journalistic purpose". However, Article 1 of the DPD is not simply a privacy directive but also provides for the protection of fundamental rights and freedoms, including privacy.[41] This includes the rights contained within the European Convention of Human Rights.[42] In other words, Article 10 of the ECHR would also be applicable. Article 9 should not be interpreted strictly and it is possible that a webpage could still fulfill the "journalistic purpose" criteria,[43] so it is not entirely clear that "journalistic purpose" could not be satisfied. As cases such as *Lindqvist* indicate, it would be a balancing act for the Member States to decide whether Article 9 (as implemented within the national laws) is applicable.[44] Within the United Kingdom, a three-pronged test is used to decide whether processing was intended for a "journalistic purpose". This is covered within s. 32 of the DPA 1998 which states "personal data which are processed for the special purposes are exempt from any provision to which this subsection relates if:

> (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."

---

[41] Article 1 of the Data Protection Directive 95/46/EC expressly provides that "in accordance with this Directive, Member State shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

[42] *See id*.

[43] An example to consider would be the Swedish Supreme Court decision in *Ramsbro*. The full extent of the court case is http://dsv.su.se/jpalme/society/Ramsbro-HD-domen.html (in Swedish). *See also* L.A. BYGRAVE *Balancing data protection and freedom of expression in the context of website publishing – recent Swedish case law*, CLSR 56 (2002); M. KLANG *Technology, speech, law and ignorance: the state of free speech in Sweden*, HERTFORDSHIRE L. J. 48 (2003).

[44] *See* ECJ Case C-101/01 *supra* note 20.

As indicated by the United Kingdom's Court of Appeal in *Campbell v. MGN*[45], s 32 DPA 1998 would be given its natural meaning, and apply before and after publication.[46] The Court of Appeal has given some direction on the application of s. 32 DPA 1998, stating it would set a high bar before s. 32 could be applied. Furthermore, the burden would be on the data controller to show that the special purpose is applicable to SNS.

While it is apparent that something must be done, the obvious question is "what?" The Data Protection Commissioners from Australia, the United Kingdom and Sweden have tried to address the complex issues concerning social networks. Several of these Data Protection Commissioners have provided frameworks[47] around the use of social networks, but they fall short in providing tangible steps on how to regulate individuals and social networks.[48]

In Australia, the Privacy Commissioner posted a media release titled "Protect your privacy on social networking sites, says Privacy Commissioner".[49] The advice from the Australian Privacy Commissioner to users of social networking websites is simply to be aware of the risks, taking a common sense approach to looking after your own personal information which includes reading the privacy policy and being careful about what personal information is given. To date, there have not been any legal cases brought in Australia relating to social networking and privacy.

The Canadian Privacy Commissioner has been proactive in warning of the dangers of using social networking websites and individuals giving away personal information.[50] The Privacy Commissioner has produced a video titled "What does a friend of a friend of a friend need to know about you" highlighting the perils of SNS.[51]

---

[45] [2002] EWCA Civ. 1373.
[46] *Id*.
[47] *See e.g.*, report of Australian Data Protection Commissioners *available at* http://www.privacy.gov.au/links/index.html, the report of the United Kingdom Data Protection Commissioners *available at* http://www.ico.gov.uk/, and the Swedish Data Protection Commissioners *available at* http://www.austlii.edu.au/catalog/279.html.
[48] This list is exemplary, and not exhaustive.
[49] The full text of the Media Release is *available at* http://www.privacy.gov.au/news/media07_print.html
[50] Posting of Colin McKay to http://blog.privcom.gc.ca/index.php/2007/10/10/social-networking-and-privacy (Oct. 10, 2007, 9:48 EST).
[51] The video is *available at* http://blog.privcom.gc.ca/index.php/privacy-on-social-networks.

Recently, four University of Ottawa law students alleged that Facebook had given their personal information to marketers without their consent.[52] The Privacy Commissioner is currently investigating this case. These legal challenges and discussions are still in progress at the time of this article.[53]

In Germany, the current developments are impacted by the German Federal Data Protection Act 2001.[54] This Act applies to federal public bodies and private organizations.[55] State ("Land") data protection laws apply 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.[56] 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.[57] It is unclear whether the Federal Data Protection Act 2001 would cover individuals who post information about other individuals which may have adverse effects, and whether this would be exempt for the purposes of "literary or journalistic purposes"? The Berlin Data Protection Commissioner[58] expressed its view pursuant to inquiry 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

---

[52] Associated Press, *Canada's Privacy Commissioner launches Facebook probe after law students file complaint*, INTERNATIONAL HERALD TRIBUNE, May 31, 2008 *available at* http://www.iht.com/articles/ap/2008/05/31/business/NA-GEN-Canada-Facebook-Probe.php.

[53] At the time of writing, a decision is expected in mid-June 2009. More details can be obtained from the CIPPIC at http://www.cippic.ca/en/.

[54] Bundesdatenschutzgesetz [BDSG] [German Federal Data Protection Act] 2001.

[55] *See id*.

[56] Handelsgesetzbuch [HGB] [German Telemedia Act] Feb. 16, 2007.

[57] *See id*.

[58] E-mail from Berlin Data Protection Commissioner's Office (Sept. 12, 2008) (on file with author).

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 published guidelines on social networking and data protection issues.[59]

According to one legal expert on data protection issues in Germany, someone who uploads material to a social networking site would be regarded as the controller of the data until it is uploaded.[60] At that point the social networking website would then become the data controller. Even if these social networking websites were to use the exemptions on the grounds of "press privileges" it would not exclude the application of the Federal Data Protection Act or the Telemedia Act. To date, there have been no actual legal cases determining the extent of the application of data protection laws to social networking in Germany.

The Personal Data Act 1998 regulates the processing of personal data in Sweden, and implements the Data Protection Directive 95/46/EC.[61] There have been guidelines issued by the Swedish Data Inspection Board on social networking.[62] On a specific point relating to the scope of a "data controller" within the definition of the DPD 95/46/EC, this question is still to be determined by the Data Inspection Board. Following questions to the Swedish Data Inspection Board ("DIB"),,[63] it has not yet had any specific cases regarding websites, nor issued any formal opinions on this subject. According to the

---

[59] *See generally The Common position of German Data Protection Oversight Authorities for the private sector ("Düsseldorfer Kreis") of April 2008 available at* http://www.datenschutz-Berlin.de/attachments /487/Düsseldorfer KreisApril 2008-Datenschutzkonforme-Gestaltung-sozialer-Netzwerke.pdf?1212737975 (in German only).

[60] Many thanks to Dr. Ulrich Wuermeling, of Latham and Watkins LLP, for his insights into this subject.

[61] *See* Council Directive 95/46 *supra* note 5.

[62] *Id*.

[63] Grateful acknowledgements to Elizabeth Wallin, Legal Advisor, Data Inspection Board, for her responses, dated 9 September 2008.

DIB, the Personal Data Act 1998 is applicable to personal data that is published by people or organizations that are established in Sweden.[64] The only difficulty that may arise is tracing the source of the information (the "infringer" for posting personal information online). The Swedish Inspection Board, however, has issued some results into a study carried out among young people at the beginning of 2008 on their views regarding Facebook.[65] According to the report, half of the young people interviewed had been subjected to someone lying or writing unfair postings about them on the internet.[66] One out of five has experienced someone else using their identity, and twenty nine percent of the queried young women say they have been subjected to sexual harassment on the Internet.[67] Eighty-six percent have published photographs of themselves.[68] However, there is a great deal of resistance to others publishing photographs without asking permission, but thirty percent have been subjected to this.[69] According to the DIB notwithstanding these offences, young people still unnecessarily reveal personal information on the internet, which would be unthinkable to do elsewhere besides cyberspace. The DIB has indicated that more needs to be done and this is expressed by DIB Member Göran Gräslund:

> Behavior 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.[70]

---

[64] *Id*.
[65] The study is available in Swedish only and is *available at* http://www.datainspektionen.se/Documents/rapport-ungdom2008.pdf.
[66] *Id*.
[67] *Id*.
[68] *Id*.
[69] *See Every other young person has been offended on the internet*, posting on http://www.datainspektionen.se/en-english/every-other-young-person-has-been-offended-on-the-internet on Data Inspection Board. (Discussing the resistance to others publishing other's private information without permission).
[70] *Id.*

The UK Information Commissioner ("ICO") has also been quite active in publishing guidelines on social networking and privacy, recommending that youth should not put too much personal information on social networking websites.[71] What is unclear is the extent to which third parties such as prospective employers; banks and even supermarkets for instance, are likely to use this information and whether these third parties have a policy in place indicating that they access social networking websites. 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. Thirty nine percent of adults have profiles on two or more sites.[72]

The Information Commissioner has reviewed complaints on social networking sites as far back as 2005. The Commissioner reported that up to 2008 they had two complaints against Bebo, five complaints against Facebook and no complaints against MySpace.[73]

The International Working Group on Data Protection in Telecommunications ("Working Party") in March 2008 published guidelines into the use of SNS and privacy, which requires some perceptive analysis.[74] It took the view that legislators, Data Protection Authorities and social network providers were faced with a situation that had no visible past.[75] The Working Group recognized that once personal information was published on the internet, it may languish there forever, even when the data subject has deleted the information from the original site.[76] The Working Group also identified that there was a misleading notion of "community" in SNS which leads individuals to readily share personal information, and that platforms (such as "MySpace") create the illusion of intimacy on the web.[77] To highlight this misperception, imagine the SNS to be more

---

[71] *See generally* ICO Guidelines referenced *supra* at note 44.
[72] *See* Swedish study *supra* note 62.
[73] *See supra* note 68.
[74] *See* Report and Guidance on Privacy in Social Network Services – "Rome Memorandum", 3-4th March 2008 available at https://www.agpd.es/portalweb/canaldocumentacion/internacional/common/pdf/wp_social_network_services.pdf. *See also* Rebecca Wong, *Social Networking: Anybody is a Data Controller!* 7-9 (Nottingham Law Sch., Working Paper, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668.
[75] Wong, R, *supra* note 11.
[76] *Id*.
[77] *Id*.

like a dinner date, where a couple speaks intimately over candlelight into a loudspeaker for all other diners to eavesdrop and hear the details. Traffic data (the details) was frequently collected by third parties, which also depended on the privacy settings that were available.[78] The Working Party also found that where employment is concerned, one third of the human resource managers admitted to using data from social networking services (now that bit of information should cause most individuals to rethink the information they give out!).[79] The Working Group was particularly concerned about the rise in identify theft through the proliferation of user profiles. The main recommendation worth noting is that service providers should be honest and clear about what information is required so that users can make informed choices as to whether to take up the service.[80] The Working Group also recommends the introduction of data breach notifications by service providers, so that users can be better informed in their choices.[81] 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.[82] The goal of this recommendation is to possibly attribute more responsibility for personal data content on social networking sites to the social networking providers.[83] The study concluded by indicating that the Working Party will closely monitor future developments, and revise and update the guidance where deemed necessary.[84] [is there anything in the recent EU framework review which is just concluding?]

The long and short of it is that today, anybody is a data controller in a social networking website, there should be refinement of legislation and a mature realisation that data protection principles need to be followed. This includes processing personal data fairly and lawfully, and ensuring that it does not exceed what is required.

---

[78] *Id*.
[79] *Id*.
[80] *Id*. at 12.
[81] *Id*. at 13.
[82] *Id*.
[83] *Id*.
[84] *Id*. *See also* discussions on social networking from the International Data Protection Commissioners' Conference 2008, held in Strasbourg at http://www.privacyconference2008.org/index.php?page_id=11#panel4.

Requiring ALL individuals to abide by the data protection principles on a SNS would be difficult to police and enforce. Two possible solutions exist. First, that the SNS provider takes more responsibility to ensure that the privacy of a user's profile is not misused by other individuals. Secondly, to consider the creation of an alternative dispute resolution process (so courts are not inundated with law suits), such as an independent arbitrator. The arbitrator will determine the social networking disputes, on the basis that the parties agree that the decisions are based on the applicable law and will be binding.[85]

Although there have been relatively few lawsuits against SNS, this is unlikely to remain the case.. With the amount of new users joining SNS daily, the "levees" are sure to break and litigation disputes between individuals claiming processing of personal information will consequently flood the courts. This has already occurred in *Lindqvist*[86] and in *Applause*,[87] which was successfully brought by one individual in the United Kingdom for posting a false profile of the user. In *Applause*, the decision did not consider the legal question of who was the data controller, which is likely to be a question of fact (*Common Services Agency v. Scottish Information Commissioner*).[88] It is apparent that the solution requires parties to resolve several leading questions such as:

- How to quantify and identify who are the data controllers?
- When does the DPD apply to social networks and individuals?
- What are appropriate enforcement mechanisms specific to social networks?
- When should the exemptions arise?

Failure to resolve these issues is likely result in an increase in litigation, which courts are neither ready nor equipped to handle.

Ultimately, consent of the individual will be the key to whether he would like his personal information aggregated to form a personal profile. If the purpose is the

[85] Any applicable exemptions will be clearly and narrowly interpreted and applied.
[86] *See Lindqvist supra* note 23.
[87] See *Applause supra at* note 9.
[88] *Common Servs. Agency v. Scottish Info. Comm'r* [2008] UKHL 47.

effectively applying the data protection laws to social networking websites, it is important that individuals and SNS certainly understand the limits of regulation and consider building in "privacy conscious" ways to protect the user's identity.

The growth of social networking websites has left the legal world in a game of "catch up." Those charged with data protection development continue to evaluate and make recommendations. Educating the younger generation and the neophyte user about the wider availability of this personal information is a good starting point. It is also understood that the data protection framework needs to be strengthened so that it is more robust with stronger remedies for breach of individual's personal information. While no solution is ideal, it is important that the data protection framework is applied in a reasonable fashion to SNS, and that the users' frustrations and concerns continue to be of importance for this consideration. Individual awareness, responsibility and assistance through education will assist in abating the unwitting hijacking transfer of private information. Because, at the end of the day "you are responsible for you" and awareness of the continuing perils of social networking should be incorporated into your daily communications and activities. Failure to maintain a high degree of awareness could easily leave you with these unanswered questions, "How could this have happened?" "Who do these people think they are?" and the worst case scenario, "Who is this person and why is he ruining my life?"

Bibliography

EDWARDS, L.C. MARSDEN & I. BROWN, *CYBERSTALKING 2l0 available at* http://www.law.ed.ac.uk/ ahrc/gikii/papers07.asp.

J. Grimmelmann, *Facebook and the social dynamics of privacy* (NYLS Legal Studies Research Paper No. 08/09-7 2009).

L.A. BYGRAVE *Balancing data protection and freedom of expression in the context of website publishing – recent Swedish case law*, CLSR 56 (2002);

M. KLANG *Technology, speech, law and ignorance: the state of free speech in Sweden*, HERTFORDSHIRE L. J. 48 (2003).

P. Seipel *Sweden in Nordic Data Protection Law* (P. Blume ed., 2001

REBECCA WONG & JOSEPH SAVIRIMUTHU, *All or nothing: the application of Article 3.2 of the Data Protection Directive 95/46/EC to the internet*, J. MARSHALL L.REV. 25 (2008)..

REBECCA Wong, *Data Protection Online: Alternative Approaches to Sensitive Data, Journal of International Commercial Law and Technology* (2007) 2(1) 9-16.

S. James, SOCIAL NETWORKING SITES: *regulating the online Wild West of Web 2.0* Ent. L.R., 19(2), 47-50 (2008).

Simitis, S. *Revisiting Sensitive Data* http://www.coe.int/T/T/Leal%5 Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/Documents/Reports/W-Report%20Simitis.asp#TopOfPage, 1999

T. Gray; T. Zeggane, W. Maxwell, *US and EU authorities review privacy threats on social networking sites*, *Ent. L.R.* 19(4) 69-74 (2008).