Brigham Young University International Law & Management Review

Volume 6 | Issue 2 Article 6

6-22-2010

Data Protection: The Challenges Facing Social Networking

Daniel B. Garrie

Maureen Duffy-Lewis

Rebecca Wong

Richard L. Gillespie

DATA PROTECTION: THE CHALLENGES FACING SOCIAL NETWORKING

*Daniel B. Garrie, Esq.**

*The Honorable Maureen Duffy-Lewis***

Rebecca Wong, Esq. †

Richard L. Gillespie, Editor††

I. INTRODUCTION

The popularity of social networking sites has increased dramatically over the past decade. A recent report indicated that thirty-eight percent of online users have a social networking profile.[1] Many of these social networking site users (SNS users) post or provide personal information over the internet every day. According to the latest OfCom study, the average adult SNS user has profiles on 1.6 sites and most check their profiles at least once every other day.[2] However, the recent rise in social

* 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.

** 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.

† 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.

†† 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.

1. *See* Richard Wray, *Social Networking Booming with Doubling of Online Profiles,* Oct. 16, 2009, *available at* http://www.guardian.co.uk/business/2009/oct/16/social-netwrkign-facebook-internet.

2. *See* Ofcom, SOCIAL NETWORKING: A QUANTITATIVE AND QUALITATIVE RESEARCH REPORT INTO ATTITUDES, BEHAVIORS & USE 5 (2008), *available at* http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf.

networking activity has opened the door to the misuse and abuse of personal information through identity theft, cyber stalking, and undesirable screenings by prospective employers.[3] Behavioral advertising programs have also misused personal information available on social networking sites.[4] Society is now facing an important question: what level of privacy should be expected and required within the social networking environment?[5]

As social networking technology has raced forward, it has left corresponding legislation in the dust. Although several countries have enacted various laws governing personal data protection to address this growing problem, these data protection laws have remained sorely inadequate to protect personal information in the social networking environment.

In this Article, we wish to focus our attention on the Data Protection Directive 95/46/EC (DPD), which the European Commission enacted in 1995. It was drafted long before the web 2.0 era, and therefore without social networking in mind. As we will explain below, strictly applying the DPD to some SNS users—in particular, those acting as "data controllers" under the DPD—is highly problematic and impractical. To understand why, we will first explain more about the DPD—namely, its definitions and what it requires of those falling under the definition of "data controller."[6]

This Article is divided into six parts. Part II will explain the background of the DPD with a focus on the definition of data controller and the obligations required by those who are considered data controllers. It will also explain the estaKblishment of supervisory authorities in each Member State and the establishment of the Article 29 Working Party. Part III will then discuss the problems inherent in strictly applying the DPD within the social networking context. Part IV will explore attempts to create a workable model for personal data protection within the social networking environment. It will explore methods several countries have used to protect personal data in the social

3. *See* Gray, Zeggane & Maxwell, *US and EU Authorities Review Privacy Threats on Social Networking Sites*, 19(4) ENT. L. REV. 69 (2008); IAN BROWN ET AL., STALKING 2.0: PRIVACY PROTECTION IN A LEADING SOCIAL NETWORKING SITE, http://www.law.ed.ac.uk/ahrc/gikii/docs2/edwards.pdf.

4. For an in-depth analysis, see SPRINGER SCIENCE, PROFILING THE EUROPEAN CITIZEN (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

5. *See generally* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOUR & PRIVACY ON THE INTERNET (2007).

6. However, as discussed *infra* Part IV.D, p. 24, the Article 29 Working Party—an organization setup under the DPD—recently published an opinion that attempts to explain the extent to which the DPD is likely to apply to social networking providers and users.

networking context and the possible utilization of several exemptions to liability found in the DPD. Part IV will also discuss the Article 29 Working Party's recently issued Opinion regarding the applicability of the DPD to social networking users. Part V will offer recommendations for going forward with data protection in the social networking realm. Finally, Part VI will summarize and conclude this Article.

II. BACKGROUND TO THE EU DATA PROTECTION DIRECTIVE

A. DPD Applies to Data Controllers

The EU enacted the DPD in 1995. The DPD regulates the processing of personal data, i.e., any information relating to an identifiable person.[7] The DPD separates those involved with the processing of personal data into two categories: "data subjects" and "data controllers." The DPD defines a data subject as the identifiable person to whom the personal data relates.[8] 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 . . . ."[9] Responsibility for compliance with the DPD rests on the data controller.

As we will discuss further in Part III below, the language defining the role of data controllers supports the view that individuals who post information about others on the internet or who use others' information found on the internet for a certain purpose would be regarded as data controllers. Thus, social networking companies, individual users, and those who use information posted on social networks could each be classified as a data controller under the DPD, and therefore could be subject to the attendant requirements.[10]

B. Supervisory Authorities and the Article 29 Working Party

The DPD requires each Member State to appoint a "supervisory authority" to monitor the application of the DPD within its territory.[11] Besides monitoring the application of the DPD in its territory, the

7. *See* Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) 31 (EC) (defining personal data as "information relating to an identified or identifiable natural person").

8. *See id.*

9. *Id.* art. 2(d).

10. *See supra* text accompanying note 6. The implication of the Article 29 Working Party's opinion is examined below in Part IV.

11. *See* Council Directive 95/46, *supra* note 7, art. 28.

supervisory authority is endowed with power either to engage in legal proceedings where national laws adopted pursuant to the DPD have been violated or to bring violations to the attention of judicial authorities.[12] Furthermore, each Member State is required to consult with the supervisory authority when drafting "administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data."[13]

The DPD also established what has become known as the Article 29 Working Party (Working Party).[14] The Working Party is partly comprised of representatives of the supervisory authorities designated by each Member State.[15] Under Article 30(1), the Working Party has a duty to:

> a)examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;
> b)give the Commission an opinion on the level of protection in the Community and in third countries;
> c)advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;
> d)give an opinion on codes Community level.[16]

Furthermore, the Working Party "may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community."[17] As will be discussed below, in June 2009 the Working Party issued an Opinion regarding the applicability of the DPD in the social networking context.

12. *See id.* art. 28.3.
13. *Id.* art. 28.2.
14. *See id.* art. 29.1.
15. *See id.* art. 29.2.
16. *Id.* art. 30.1.
17. *Id.* art. 30.3.

III. PROBLEMS APPLYING THE DPD IN THE SOCIAL NETWORKING CONTEXT

Under a strict reading of the DPD, both social networking providers and users are likely subject to the responsibilities of data controllers. Social networking providers are clearly data controllers as defined by the DPD because they "determine the purposes and means of the processing of personal data" by providing a social networking platform in the first place.[18] The purpose for processing the personal data is usually to allow users to engage in social networking so that advertisers can use information posted on user profiles to better target their ads. The means for processing personal data is determined by the provider based on the setup and organization of the social networking site.

However, under the DPD individual social networking users are also likely to be considered data controllers because they too "determine the purposes and means of the processing of personal data."[19] Social networking users post personal data or information about others on their own user profiles or on their friends' profiles using text, photographs, and video. Each user has a purpose for posting (or processing) personal data and chooses how (the means) it is to be posted. Thus, although individual SNS users could be classified as data controllers, imposing the requirements of data controllers on them without modification does not seem practical under the DPD. Such a classification raises multiple questions and problems.

This section will (1) highlight the differences between *organizational* data controllers (such as MySpace, Facebook, and Twitter) and *individual* data controllers (such as SNS users) to illustrate the impracticability of applying the DPD to SNS users, and (2) point out the possibility of widespread liability and litigation that is likely to ensue if the DPD is strictly enforced against SNS users.

A. Impracticability of Applying the DPD to Individuals in the Social Networking Context

The differences between typical organizational data controllers and individual data controllers operating in the social networking context make strict application of the DPD difficult. As explained above, individuals who either post another person's information on their own profile or use information found on another person's profile would be

18. *Id.* art. 2(d).
19. *Id.*

deemed data controllers and would therefore be subject to the obligations imposed on data controllers by the DPD. Obligations for data controllers are littered throughout the DPD. For the purpose of this Article, only a few are mentioned here. As explained below, applying these obligations to individual users would be highly impractical, if not impossible.

First, the DPD requires that data controllers process all data lawfully and fairly.[20] To require every user (as a data controller) to do this within a social networking environment would be an unrealistic objective. It is difficult to imagine the effects of requiring all individual SNS users to consult the laws of his or her country and accurately determine whether or not the information in a particular post is lawful and fair before posting it. After a period of adjustment, it is plausible that SNS users would become familiar with the body of law applicable to the types of posts that they routinely make on social networking sites. However, even if the public were largely successfully at becoming familiar with the mandates of this requirement, policing and monitoring would be very difficult for the Supervisory Authorities because of the incredible number of users that exist.

Second, the DPD requires that data controllers supply data subjects with certain information, such as (1) "the identity of the controller," (2) "the purposes of the processing for which the data are intended," and (3) "the recipients . . . of the data."[21] It is customary for an organizational data controller to provide this type of information to the data subject; however, it is less customary, if not unheard of, for a SNS user to do so. For example, a company would likely provide this information to a data subject in order to gain trust and entice them to supply personal information. However, SNS users usually have no need to entice data subjects to supply personal information because oftentimes SNS users already have the data subject's personal information under their control. Furthermore, it is nearly impossible for a SNS user to determine who will receive a subject's personal data because the information users post is often public and accessible to the entire world.

Third, the DPD requires that information collected by data controllers concerning data subjects be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or for which they are further processed."[22] Again, this provision is more applicable to an organization. It would be unusual to require a SNS user

20. *See id.* art. 6.1(a).
21. *Id.* art. 10.
22. *Id.* art. 6.1(c).

to determine whether he has necessarily provided information about other individuals that is "adequate, relevant and not excessive," since the user himself provides the information and determines the purpose for which data is processed. In other words, the SNS user determines the scope of his or her profile and the information it contains.

Finally, in addition to the aforementioned rules, the DPD not only requires that a data controller obtain the data subject's consent to process the data subject's personal data, but also that the data controller obtain consent for the specific purpose for which that data is being processed.[23] It would be impractical to require SNS users to fulfill this consent requirement. In the social networking realm, it is not customary to ask permission before posting another's personal information, such as a photo or video. Although some data subjects may have consented to the processing of personal data by posting personal information on their own profile, this does not mean they have necessarily consented to have fellow SNS users process this data. In other words, it is likely that the data subject may have only consented for one purpose[24]—namely, to have the data available only to a limited group to which the user has granted access—not to have it available to those who have access to another SNS user's profile, other third parties, employers, or the wider public.

It is unwise to require SNS users to comply with the obligations that the DPD requires of data controllers as presently constituted. The numerous obligations of data controllers, not to mention others which are not discussed here, make it easy to see why a SNS user might be discouraged from posting information about others. Also, strict enforcement of the DPD (or corresponding national data protection laws) as applied to SNS users remains uncertain because personal information is readily available on social networking sites and many users have already consented to have this information accessible to others.[25] Furthermore, it defeats the original purpose of the DPD, which was originally legislated to address the copious amount of personal data processed electronically by organizations rather than by individuals.

Questions which remain unanswered and that must be considered by the E.U. in the future are:

23. *See id.* art. 7(a).

24. *See generally* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) (discussing SNS in-depth).

25. *Cf.* Council Directive 95/46, *supra* note 7, art. 7–8 (requiring "unambiguous" consent for the processing of normal data per article 7(a) of the DPD and "explicit consent" under Article 8 for the processing of special categories of data).

1)Would it be fair or practical to hold individuals who post information and photographs about friends and family to the strict requirements of "data controllers" under the DPD?
2)Should the obligations and consequences for individuals be the same at all times as those for organizations?
3)Should a new category be created for individual data controllers with obligations adjusted accordingly? Would such a category be feasible?
4)Would application of the DPD to SNS users stifle social networking because individuals would not want to go through the trouble of understanding and complying with DPD provisions? Conversely, would application of the DPD have a positive effect—a heightened awareness of user responsibilities in a user-generated environment?

B. Liability and Enforcement

With millions of SNS users, the current liability of user-generated content under the DPD is potentially limitless. It is unclear whether the DPD is a suitable framework for resolving civil disputes involving the misuse of personal information. The E.U. must re-evaluate the direction of the DPD as it applies to social networking in order to better protect individuals and prevent the potential rise of litigation.[26]

Questions that need to be considered by the E.U. in the future are:

1)How easily and how often is personal data (and potentially false data) about others circulated?
2)Should there be an opportunity to remedy any resulting damage? If such an opportunity exists, then to whom and how far should liability extend?
3)Should the DPD (or national data protection laws) be enforced strictly, considering that personal information is readily available on social networking sites and that users have

26. *See generally Resolution on Privacy Protection in Social Network Services*, 30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, Oct. 17, 2008, *available at* http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf (espousing, by way of resolution, recommendations of a panel, convened in October 2008 at Strasbourg, Germany, regarding SNS; main recommendations include: more user control of profile data, data security through default privacy settings, easy termination of user profiles, the creation and use of pseudonymous profiles as an option, and that external search engines have the ability to index user profiles only when a user has given explicit, prior, and informed consent).

consented to have this information accessible to others?[27]

4) When complications arise, should the DPD be enforced by Data Protection Authorities, by private right of action, or by some other means?

In sum, the social networking structure creates difficulties and challenges for applying the DPD because it imposes responsibilities on individuals (not only organizations) regarding how they use information about others. Whether liability under the DPD is a suitable or preferred method for resolving civil disputes involving the posting/publication of personal data on profiles is even less clear. Furthermore, it is not yet certain whether the DPD will be strictly enforced against SNS users by Data Protection Authorities or by a private right of action when complications arise.

IV. ATTEMPTS TO CREATE A WORKABLE MODEL FOR PERSONAL DATA PROTECTION IN THE SOCIAL NETWORKING ENVIRONMENT

From a discussion of the inherent problems of a strict application of the DPD in the social networking context naturally follows an analysis of what attempts are being made to solve these problems. This section will (1) take a look at the various approaches which have been taken in several countries to implement and apply the DPD in the social networking environment, (2) review the recommendations made by the International Working Group on Data Protection in Telecommunications (Working Group), (3) consider the possible utilization of liability exemptions found in the DPD, and (4) discuss the Working Party's recently published Opinion concerning the DPD and social networking related issues.

A. Different Approaches Taken by Various Countries

The Privacy Commissioners from Australia, Canada, Germany, Sweden, and the United Kingdom have all tried to address the complex issues concerning social networks. Several of these countries have provided frameworks[28] around the use of social networks, but some fall

27. *See* Council Directive 95/46, *supra* note 7, art. 7–8 and accompanying text.

28. *See, e.g.*, Australian Government: Office of the Privacy Commissioner, http://www.privacy.gov.au/index.php (last visited Apr. 15, 2010); United Kingdom: Information Commissioner's Office, http://www.ico.gov.uk/ (last visited Apr. 15, 2010); and Australasian Legal Information Institute: Privacy Protection Agencies, http://www.austlii.edu.au/catalog/279.html (last visited Apr. 15, 2010).

short in providing tangible steps to regulate individuals within the social networking context.[29]

1) Australia

In Australia, the Privacy Commissioner posted a media release titled "Protect Your Privacy on Social Networking Sites."[30] The release urges users to be aware of the risks associated with using social networking sites and advises them to take a common sense approach to protecting their personal information. This includes reading the privacy policy and being careful about what personal information is shared. Although the Privacy Commissioner has warned SNS users of possible conflicts associated with posting personal information on these sites, it does not appear that Australia has set forth any specific regulations pertaining to social networks. To date, there have not been any legal cases brought in Australia related to social networking and privacy.

2) Canada

In Canada, the Privacy Commissioner has proactively warned citizens of the dangers associated with sharing personal information on social networking sites.[31] For example, the Privacy Commissioner produced a video titled, "What Does a Friend of a Friend of a Friend Need to Know About You" highlighting the perils of social networking.

Recently, four University of Ottawa law students submitted a complaint before the Privacy Commissioner alleging that Facebook had given their personal information to marketers without their consent.[32] In July 2009, the Privacy Commissioner issued a decision regarding this case in which the Commissioner concluded that Facebook needed to improve its privacy practices to comply with Canada's privacy laws.[33] The Commissioner also determined that the allegations against Facebook concerning misrepresentation, deception, and Facebook Mobile were not well-founded. However, the Privacy Commissioner held that the allegations concerning third-party applications, account deactivation and

29. This list is exemplary, not exhaustive.

30. The full text of the Media Release is available at http://www.privacy.gov.au/news/media07_print.html.

31. Posting of Colin McKay to Office of the Privacy Commissioner of Canada, http://blog.privcom.gc.ca/index.php/2007/10/10/social-networking-and-privacy (Oct. 10, 2007).

32. Associated Press, *Canada Launches Privacy Probe Into Facebook*, USA TODAY, May 31, 2008, http://www.usatoday.com/news/world/2008-05-31-1179330323_x.htm.

33. Additional details can be found on the CIPPIC website available at http://www.cippic.ca/en/.

deletion, accounts of deceased users, and non-users' personal information were in breach of the PIPEDA Act.[34] The Assistant Commissioner further held: "Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers."[35] Facebook was given thirty days to implement measures to rectify these problems.[36] This Canadian decision exemplifies how countries might regulate the use of personal data on social networking sites.

3) Germany

In Germany, the current developments involving social networking sites, data controllers, and online activities are impacted by the German Federal Data Protection Act 2001 (German FDPA).[37] This Act applies to federal public bodies and private organizations.[38] The German Telemedia Act regulates online activities.[39] Under the German

34. *See* ELIZABETH DENHAM, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CENTER (CIPPIC) AGAINST FACEBOOK, INC. UNDER THE PIPEDA (2009), *available at* http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf; *see also* Michael Geist, *Privacy Commissioner Finds Facebook Violating Canadian Privacy Law,* July 16, 2009, http://www.michaelgeist.ca/content/view/4139/125/; Robin Wauters, *Canadian Privacy Commissioner says Facebook is Full of Holes,* July 16, 2009, http://techcrunch.com/2009/07/16/canadian-privacy-commissioner-says-facebook-is-full-of-holes/.

35. DENHAM, *supra* note 34, at 3.

36. *See id.* at 4.

37. Bundesdatenschutzgesetz [BDSG] [German Federal Data Protection Act] May 22, 2001, BGBI. I at 904 (F.R.G.); the Federal Data Protection Act has recently been amended to strengthen the Data Protection Act, but those changes are not considered here. For more information, see generally Robert Alan Heym et al., *Germany: Changes to the German Federal Data Protection Act: An Overview,* MONDAQ, Apr. 7, 2009, http://www.mondaq.com/article.asp ?articleid=76712.

38. *See id*.

39. *See generally* Telemediengesetz [TMG] [German Telemedia Act] Feb. 16, 2007 BGBI. I at 179 (F.R.G.). Detailed analysis of the German Telemedia Act is provided by Professor Thomas Hoeren, *Das Telemediengesetz,* Mar. 19, 2007, http://128.176.101.170/hoeren_veroeffentlichungen/telemediengesetz.pdf (only available in German). *See also* Henning Krieg, *German Telemedia Act Introduces New Rules for New Media,* Mar. 5, 2007, http://www.twobirds.com/English/News/Articles/Pages/German_Tele_Media_Act_new_rules.aspx; Alexander Scheuer, *Telemedia Act Adopted,* http://merlin.obs.coe.int/iris/2007/3/article17.en.html (last visited Mar. 6, 2010); Hunton and Williams LLP, *German Data Protection Authorities Issue Resolution on Website Analysis Methods,* Jan. 7, 2010, http://www.huntonprivacyblog.com/2010/01/articles/european-union-1/german-data-protection-authorities-issue-resolution-on-website-analysis-methods/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PrivacyInformationSecurityLawBlog+%28Privacy+%26+Information+Security+Law+Blog%29).

Telemedia Act, social networking sites fall within the scope of the German FDPA unless user profiles on the sites are made strictly private.[40] The German FDPA is likely to apply to social networking providers,[41] but is unclear as to whether the FDPA would extend to SNS users who post information about others and whether this use of personal information would be exempted by the "literary or journalistic purposes" or "private purposes" exemptions found in the FDPA.[42] The Berlin Data Protection Commissioner, who publishes guidelines on social networking and data protection issues,[43] expressed his view as to whether SNS users qualify as data controllers as follows:

> Whether a subscriber would be held as a controller of such [third party personal] 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*.[44]

Another legal expert on data protection issues in Germany expressed a slightly different view. According to Dr. Ulrich Wuermeling, a SNS user who uploads material to a social networking site would be regarded as the controller of the data until it is uploaded.[45] Once the data is

40. *See* German Telemedia Act, *supra* note 39.

41. *See Data Protection Commissioner Warns over Social Networking Sites*, Dec. 27, 2009, http://www.dw-world.de/dw/article/0,,5060457,00.html; *see also Facebook Comes under German Law,* Feb. 20, 2010, http://www.thelocal.de/sci-tech/20100220-25389.html.

42. *See* "Literary or Journalistic Purposes" exemption under the DPD is discussed *infra* Part IV.C.2.

43. *See generally* The International Working Group, *The Common Position of German Data Protection Oversight Authorities for the Private Sector ("Düsseldorfer Kreis")* (April 2008), *available at* http://www.datenschutz-Berlin.de/attachments /487/Düsseldorfer KreisApril 2008-Datenschutzkonforme-Gestaltung-sozialer-Netzwerke.pdf?1212737975 (only available in German).

44. E-mail from Berlin Data Protection Commissioner's Office (Sept. 12, 2008) (on file with author) (emphasis added).

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

uploaded, the social networking provider would become the data controller. Even if these social networking providers invoked the "literary or journalistic purposes" exemption it would not prevent the application of the German FDPA or the Telemedia Act. To date, there are no legal cases in Germany that test either of these opposing views or that determine the extent to which data protection laws apply to social networking providers in Germany.

4) Sweden

In Sweden, the Personal Data Act of 1998 regulates the processing of personal data and implements the DPD.[46] The Swedish Data Inspection Board (SDIB) has issued guidelines for the protection of personal data in the social networking context, but has yet to clearly establish the scope of a data controller under the DPD. According to the SDIB, the Personal Data Act 1998 only regulates personal data that is published by people or organizations that are established in Sweden. However, a major problem with this geographic approach to personal data protection is tracing the source of the offending information. At any rate, like its German counterpart, the SDIB has yet to hear any personal data protection cases involving social networking sites and has yet to issue any formal opinions on the subject.[47]

Despite the lack of litigation and issuance of formal opinions, the SDIB has done more than rest upon its laurels. At the beginning of 2008, the SDIB surveyed young adults and teenagers in an attempt to better understand their experiences with Facebook.[48] According to the results, half of those surveyed reported that they had been portrayed falsely or unfairly on the internet.[49] One out of every five had been victims of identity theft on the internet. Twenty-nine percent of the young women had been sexually harassed on the Internet.[50] Eighty-six percent of those surveyed reported that they have published photographs of themselves[51] and, surprisingly, thirty percent of those surveyed reported that another

46. *See* Swedish Personal Data Act of 1998, *available at* http://www.sweden.gov.se/content/1/c6/01/55/42/ b451922d.pdf.

47. Telephone Interview with Elizabeth Wallin, Legal Advisor, Data Inspection Board (Sep. 9 2008).

48. *See* PETER SILJERUD ET AL., UNGDOMAR OCH INTEGRITET (2008), http://www.datainspektionen.se/Documents/rapport-ungdom2008.pdf (available only in Swedish).

49. *See id.* at 8.

50. *See id.*

51. *See id.* at 9; *see also Every Other Young Person Has Been Offended on the Internet*, http://www.datainspektionen.se/in-english/every-other-young-person-has-been-offended-on-the-internet/ (last visited Mar. 8, 2010) (discussing that there is a great deal of resistance to others publishing photographs without asking permission).

user had published a photograph of them without their permission. According to the SDIB, despite these negative experiences, young adults and teenagers continue to reveal personal information on the internet. An SDIB member, Göran Gräslund, indicated that more needs to be done to make young adults and teenagers more cautious when revealing personal information on the internet:

> 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.[52]

While Sweden has identified the importance of instructing everyone, especially young adults, of being cautious about providing personal information, Sweden has yet to take the more proactive step of establishing regulations regarding the protection of personal data in the social networking context.

5) United Kingdom

In the United Kingdom, the Information Commissioner (ICO) recently reviewed complaints on social networking sites. Dating back to 2005, it was revealed that there were only two complaints made against Bebo, five complaints against Facebook, and no complaints against MySpace.[53] The ICO has determined that individuals generally will not be classed as data controllers within the Data Protection Act 1998, and that even if this were not the case, the existing exemptions under section 32—the recreational and journalistic purposes exemptions—would likely apply. Furthermore, the ICO, like the SDIB in Sweden, has actively published guidelines on social networking and privacy. He recommends that youth refrain from revealing too much personal information on social networking sites.[54]

Moreover, in one significant case, *Applause Store Productions, Ltd. and Matthew Firsht v. Grant Raphael* (*Applause*),[55] the claimant brought a legal action against a former friend who posted a false profile of the

52. *Every Other Young Person Has Been Offended on the Internet, supra* note 51.

53. Written Correspondence from ICO (Sept. 2008) (on file with author).

54. *See generally* United Kingdom: Information Commissioner's Office, http://www.ico.gov.uk/Youth/section3/ intro.aspx (last visited Mar. 9, 2010).

55. Applause Store Prod. Ltd. v. Raphael, [2008] EWHC 1781 (QB).

claimant on Facebook.[56] The Court found for the claimant on the grounds of "misuse of private information."[57] However, the Court should also have held the social networking provider liable under the DPD because there was no question that some of the statements posted on the Facebook profile were defamatory and sensitive personal information.[58]

Another issue addressed in the United Kingdom is the extent to which third parties (such as employers, banks, and supermarkets) are likely to use personal information posted on social networking sites to take a peek at the private details of those with whom they deal or may deal, and whether these third parties should give notice that they access this information on social networking sites. This corollary point will need to be addressed in order to make meaningful progress in the future.

In summary, while these countries have realized the importance of warning their citizens about posting information on social networking sites, they each lack legislation addressing the consequences that await SNS users who post other individual's personal data.

B. The International Working Group

The International Working Group on Data Protection in Telecommunications (Working Group) is another body to which we should look to find recommendations on the application of the DPD to social networking. In March 2008, the Working Group published guidelines for the protection of personal data related to social networking.[59] They took the view that legislators, Data Protection Authorities, and social network providers were faced with a situation that had no visible past.[60] The Working Group recognized that once personal information is published on the internet, it may languish there forever, even when the data subject has deleted the information from the original site.[61] The Working Group identified a misleading notion of "community" and "intimacy" on social networking sites that encourages individuals to share personal information.[62] This misperception is comparable to a dinner date where a couple believes that they are

56. *See id.* at 1, 3.

57. *Id*. at 68.

58. This assumes that this type of posting constitutes the processing of personal data within the DPD.

59. *See* Rebecca Wong, *Social Networking: Anybody is a Data Controller!* 7–9 (Nottingham L. Sch., Working Paper, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668.

60. *Id.* at 11.

61. *Id.*

62. *Id.*

speaking intimately over candlelight but in reality their conversation is being amplified through a loudspeaker for all other diners to hear. Some information is capable of collection by third parties depending on the privacy settings on individual user profiles.[63] In fact, the Working Group found that one-third of human resource managers admitted to using data from social networking sites when evaluating prospective employees.[64]

The Working Group was particularly concerned about the rise in identity theft through the proliferation of user profiles. To better protect personal information, the Working Group recommends that social networking providers collect and display as little personal information as possible and that they inform users about what personal information is required before users register for their services.[65] The Working Group also recommends that social networking providers implement data breach notification services in order to provide users with a better understanding of the risks associated with particular social networking sites.[66] The Working Group further recommends that lawmakers attribute more responsibility to social networking providers regarding the protection of personal data.[67] The Working Group will closely monitor future developments and revise and update the guidance when it deems necessary.[68] These recommendations by the Working Group should be a good starting point for social network regulation, but many other issues still need to be addressed because of the ability people have to post information about others on social networking sites.

C. Exemptions Under the DPD

As is typical for most directives, the DPD contains a list of carefully drafted exemptions that provide circumstances where the DPD does not apply. However, these exemptions were not specifically drafted with social networking in mind. As a result, the practical workability of these exemptions within the context of social networking is unclear and may produce potentially undesirable side effects. Four exemptions found in the DPD are discussed below. While the DPD does not give titles to any of the following exemptions, for the purposes of this Article they will be known as (1) the private purposes exemption, (2) the journalistic purposes exemption, (3) the jurisdictional scope exemption, and (4) the

63. *Id.*
64. *Id.*
65. *Id.* at 12.
66. *Id.*
67. *Id.*
68. *Id.*

"catchall" exemption.

1) Private purposes exemption

Found in Article 3.2 of the DPD, the private purposes exemption provides that any "processing of personal data" for "a purely personal or household activity" will fall outside the scope of the Data Protection Directive.[69] Proper application of this exemption within the social networking context is tenuous at best. Necessarily, recent opinions and court cases have attempted to address the problem.

The issuance of Opinion 5/2009 on Online Social Networking (Opinion) by the Article 29 Data Protection Working Party (Working Party) clarified the application of the private purposes exemption[70] to social networking sites.[71] For example, the Opinion specifically noted that certain activities on social networking sites, such as collaboration and networking for political, charitable or professional purposes, would not fall under the private purposes exemption. Additionally, the private purposes exemption may not apply to individuals who post personal information on social networking sites that is accessible beyond self-selected contacts.[72] The decision of the European Court of Justice (ECJ) in the criminal proceeding against Bodil Lindqvist is consistent with this view.[73] Nevertheless, individuals who post information publicly will argue and probably expect that most information posted on the internet should fall under the private purposes exemption.[74]

2) Journalistic purpose exemption

Similar to the application of the private purposes exemption, application of the journalistic purposes exemption remains somewhat

69. Council Directive 95/46, *supra* note 7, art. 3.2.

70. In the Working Party's Opinion, this exemption is referred to as the "household exemption." *See* Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking*, § 3.1, at p. 5, WP 163 (June 12, 2009) [hereinafter WP 163].

71. See *infra* Part IV.D, for further discussion regarding the application of article 3.2 in connection with the Working Party's Opinion.

72. *See* WP 163, *supra* note 70, §§ 3.1.1–.2. *But see infra* note 85, § 36 (reflecting that domestic purposes includes "recreational purposes" and thus would possibly warrant that private web-pages would be brought within this scope).

73. *See* Case C-101/01, Sweden v. Lindqvist, 2003 E.C.R. I-12971, ¶¶ 42–47 (holding that Article 3.2 would be inapplicable in a situation where personal information is accessible by anyone on the Internet, rather than by a limited number of self-selected contacts); *see also* Rebecca Wong & Joseph Savirimuthu, *All or Nothing: The Application of Article 3.2 of the Data Protection Directive 95/46/EC to the Internet*, 25 JOHN. MARSHALL J. COMPUTER & INFO. L. 211 (2008).

74. *See generally* PETER SEIPEL, SWEDEN IN NORDIC DATA PROTECTION LAW (Peter Blume ed., 2001).

unclear within the social networking context. Article 9 of the DPD provides exemptions from liability for the processing of personal data carried out "solely for journalistic purposes or the purpose of artistic or literary expression."[75] However, this exemption seems to be in direct opposition to the aims of the DPD enumerated in Article 1—namely, to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[76] These fundamental rights and freedoms include those contained within the European Convention of Human Rights (ECHR).[77] Thus, Article 10 of the ECHR would also be applicable. Nonetheless, as demonstrated by the divergent approaches of Sweden and the United Kingdom, safety from liability is not entirely certain for an SNS user trying to claim the journalistic purposes exemption.

Sweden has taken the stance that Article 9 of the DPD should not be interpreted strictly, and found that a webpage could still fulfill the journalistic purposes criteria.[78] Accordingly, if a webpage can qualify for the journalistic purposes exemption, it is possible that a social networking site could as well. Thus, Sweden takes a broad view of the journalistic purposes exemption.

Expounding upon Sweden's approach, consider the following likely scenario: X works as a journalist and has a blog for reporting his current daily activities. X also uses Facebook and Twitter to relay his activities to friends and colleagues. What is Article 9's potential application?

Under such a fact scenario, it is likely that any reference that X makes to certain individuals as part of his report on a blog is likely to be covered under Article 9 (or corresponding national legislation). This might also extend to simple bloggers who are blogging as a second job. In some instances, bloggers may choose to use pseudonyms to protect themselves from liability. However, recent changes in the United Kingdom law have indicated that bloggers who use a pseudonym are unlikely to receive any protection if their identity is revealed by a third party source.[79] Accordingly, bloggers who are employed by companies

75. Council Directive 95/46, *supra* note 7, art. 9.

76. *Id.* art. 1.

77. *See id.*, Recitals ¶ 10.

78. An example to consider would be the Swedish Supreme Court decision in *Ramsbro, available at* http://dsv.su.se/jpalme/society/Ramsbro-HD-domen.html (in Swedish); *see also* Lee A. Bygrave, *Balancing Data Protection and Freedom of Expression in the Context of Website Publishing— Recent Swedish Case Law*, 18 COMPUTER LAW & SECURITY REPORT 56 (2002); M. Klang, *Technology, Speech, Law and Ignorance: The State of Free Speech in Sweden*, 48 HERTFORDSHIRE L. J. 7, 7–9 (2003).

79. *See* Author of a Blog v. Times Newspapers Ltd., [2009] EWHC (QB) 1358 (reflecting that a blogger whose blog is in the public domain does not have a legally enforceable right to

should keep in mind that company vetting opens up the possibility that their identities may be divulged without their consent.

Furthermore, cases such as *Lindqvist* indicate that Member States may employ a balancing test to decide whether Article 9 (as implemented within the national laws) is applicable.[80] For example, within the United Kingdom, the Data Protection Act 1998 (DPA) lays out a three-pronged test to decide whether processing was intended for "journalistic purposes." Section 32 of the DPA states:

> [P]ersonal 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.[81]

The U.K. Court of Appeal, in *Campbell v. MGN*, indicated that section 32 DPA 1998 would be given its "natural meaning and the only meaning that makes sense" and would "apply both before and after publication,"[82] giving some direction on the application of a journalistic purposes exemption. In other words, the United Kingdom chose to set a high bar before the journalistic purposes exemption could be claimed and leaves the burden on the data controller to show that the special purpose is applicable to the social networking site. Thus, although one Member State in the European Union has tightened the applicability of the journalistic purposes exemption, another has potentially expanded it. Therefore, the applicability of the journalistic purposes exemption

anonymity in the U.K. because the grounds for confidentiality have not been satisfied).

80. *See* Case C-101/01, Sweden v. Lindqvist, 2003 E.C.R. I-12971, ¶¶ 89–90.

81. Data Protection Act 1998, 1998, c. 29, § 32 (U.K.), *available at* http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

82. Campbell v. MGN Ltd., [2002] EWCA (Civ) 1373, [121] (Eng.), *rev'd on other grounds*, [2004] UKHL 22.

remains largely uncertain.

3) Jurisdictional scope exemption

If purpose exemptions cannot be obtained, a data controller may attempt, through the location of his activities or equipment, to fall under the jurisdictional scope exemption found in Article 4 of the DPD. [83] Article 4 outlines the territorial jurisdiction of the DPD.[84] Thus, the applicability of the jurisdictional scope exemption depends on where the data controller is based. DPD 4(1)(a) provides that the DPD (or corresponding national data protection laws) applies to *activities* of an establishment of the controller which are within the territory of the Member State.[85]

Moreover, DPD 4(1)(c) expands this jurisdiction to include areas where *equipment* is used to process such information (more difficult to show that the user-generated content falls outside the European Economic Area).[86] For example, because MySpace has an office in the United Kingdom, MySpace is considered a data controller established in the United Kingdom when data is processed in the context of that establishment or when MySpace uses equipment to process data in the United Kingdom. Thus, to take advantage of the jurisdictional scope exemption, data controllers may only need to relocate residence or equipment so that their activities fall outside the jurisdiction of the DPD.

4) The catchall exemption: Article 13

Most thoughtfully crafted laws incorporate a provision that allows an escape hatch or "catchall" in the event of unforeseen situations. The DPD's catchall exemption is found in Article 13. It states:

> Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1),[87] 10,[88] 11(1),[89] 12,[90] and 21[91] when such

83. *See* Council Directive 95/46, *supra* note 7, art. 4.

84. *See id.*

85. *See id.* art. 4.1(a).

86. *See id.* art. 4.1(c).

87. *See id.* art. 6.1 (enumerating the data protection principles).

88. *See id.* art. 10 (listing the information to be given to the data subject in cases of collection of data from the data subject).

89. *See id.* art. 11 (listing the information to be given to the data subject in cases where the data have not been collected from the data subject).

90. *See id.* art. 12 (providing for rights of access to data subject's concerning the processing of their personal data).

> a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defense; (c) public security; (d) prevention, investigation, detection and prosecution of criminal offenses, or of breaches of ethics for regulated professions; (e) an important economic or financial interest; (f) a monitoring, inspection or regulatory function connected with the exercise of official authority; and (g) *protection of the data subject or of the rights and freedoms of others*.[92]

Safeguarding the "protection of the data subject or of the rights and freedoms of others" is so general that it effectively creates a catchall. Such an exemption could potentially be twisted to fit almost any agenda. If no other exemption is obvious, social networking sites are likely to seek this final catchall exemption. Thus far, there have been no cases to clarify the scope of this final exemption. As with each of the previously mentioned exemptions, the applicability of the catchall exemption within the social networking context remains uncertain.

D. Article 29 Working Party's Opinion on Social Networking

In response to the uncertainty inherent in applying the DPD within the context of social networking, the Article 29 Data Protection Working Party recently issued an Opinion[93] not only clarifying key definitions, but also the application of the previously mentioned DPD exemptions. In response to their clarifications, several steps should be taken in order to comply with their recommendations.

In its Opinion, the Working Party defined social networking sites as "information society services."[94] And, according to the Working Party, a social networking provider would be regarded as a "data controller."[95] Application providers may fall within the scope of a data controller.[96]

As a clarification to the application of Article 3.2 of the DPD, the Working Party indicated that there are certain instances when users will be found to fall outside the protections of the private purposes

91. *See id.* art. 21 (providing for the requirement for the processing of personal data in registers).

92. *Id.* art. 13.

93. *See* WP 163, *supra* note 70.

94. *Id.* § 2.

95. *See id.* § 3.1, at 5.

96. *See id.* A good example of an application provider would be the Beacon program available on Facebook.

exemption. For instance, an SNS user will not benefit from the private purposes exemption where he "acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals."[97] Accordingly, profile information provided to an audience wider than a self-selected contacts list likely falls within the scope of the DPD.[98] The Article 29 Working Party Opinion has advised that under those circumstances default settings favoring privacy should be applied.[99] Additionally, even if Article 3.2 is not applicable, then "other exemptions such as the exemption for journalistic purposes, artistic or literary expression" may still be available.[100]

Furthermore, the Article 29 Working Party has emphasized that "a balance needs to be struck between freedom of expression and the right to privacy."[101] The following suggested steps are ways to minimize the risk of contravening the national data protection laws. Social networking providers should, at a minimum, provide:

1)Default privacy settings;
2)Inform users of the privacy risks of uploading third party information;
3)Make it clear to users that they need not submit sensitive data;
4)Provide a mechanism whereby users can report concerns about
5)applications;
6)Personal data of users should not be kept after user account is deleted; and
7)Give users and non-users the ability to change or delete personal data.[102]

SNS users should:

1)Obtain explicit consent to post personal data of a third party;[103] and
2)Have private profiles.[104]

97. WP 163, *supra* note 70, § 3.1.1.
98. *See id.* § 3.1.2.
99. *See id.*
100. *Id*.
101. *Id*.
102. *See id.* §§ 3.2-3.6; *see also id.* § 5, ¶¶ 7–15.
103. *Id.* § 3.4.
104. *Id.* § 3.2.

The Article 29 Working Party has also indicated in their opinion that three distinctions should be made in the context of direct marketing aimed at users. These include:

1)Contextual marketing;
2)Segmented marketing aimed at a specific user group; and
3)Behavioral marketing—advertisements based on their observation and analysis of user's activity over time.[105]

The Article 29 Working Party's view is that sensitive data should not be used in "behavioural advertising models, unless all legal requirements are met."[106] They have further advised that pictures or information about other individuals should only be uploaded with the user's consent.[107] Furthermore, the homepage of the social networking site should contain links to a complaint forum indicating data protection issues.[108]

The recommendations submitted by the Article 29 Working Party are helpful, but counterintuitive in a way. In practicality, the expectations required of social networking providers to fulfill their responsibilities under the DPD are more easily fulfilled compared to the expectations required of SNS users who do not qualify for the Article 3.2 private purposes exemption. Should such a seeming inconsistency and injustice prevail in our current data protection laws?

Since it was first passed in 2005, application of the DPD has raised questions over whether or not it is meeting its original aims. Even with guidance from the Article 29 Working Party, we are still considering these questions. We should consider whether SNS users' ought to be governed by the current data protection laws in the face of social norms which allude to acceptable standards. For instance, a reasonable expectation to permit the use of personal information arises when an individual becomes a member of a group or an association (e.g., clubs, university class seminars, or research groups). Uploading information about these individuals becomes an expected part of that association's work. If the DPD and corresponding national data protection laws are applied rigidly, the DPD appears to be over-protective and appears to demand too much of SNS users who do not fall within the private purposes exemption. The DPD has been criticized for being "excessive" and "burdensome." Perhaps social norms and agreement to terms and

105. *Id.* § 3.7.
106. *Id.*
107. *See id.* § 5, ¶ 11.
108. *Id.* § 5, ¶ 12.

conditions of acceptability provided by a social networking provider should be sufficient.[109]

V. RECOMMENDATIONS

The existent problems in applying the DPD to social networking sites may appear insurmountable now, but there are ways to ameliorate the current climate of uncertainty and provide a workable system. The thrust of the problem is that today, nearly anyone on a social networking site could be classified as a "data controller." Requiring *all* individuals to abide by the data protection principles in such an environment would be difficult to police and enforce. The Article 29 Working Party Opinion has clarified the extent to which individuals are able to benefit from the Article 3.2 exemption and therefore potentially minimize lawsuits, but there are still gray areas where Article 3.2 may not apply. Social networking providers should ensure that SNS users are made fully aware of this. Given that Article 3.2 only applies in limited circumstances, this provision should be revised to include "non-commercial purposes" to allow for a broader context. Any changes to the Directive, however, would have to be achieved at a European Union level. A few possible solutions exist that could create a workable system.

First, lawmakers should place more responsibility on social networking providers to ensure that the personal information of users is not misused by other individuals. Any refinement in legislation should include a mature realization that data protection principles need to be followed. This includes processing personal data lawfully and fairly,[110] and ensuring that requirements are not excessive in their scope. The interpretation, application, and harmonization of key legal concepts within the DPD, including national data protection laws as applied to social networks, will need to be considered by the national courts. The ECJ has begun this process with *Lindqvist*.

Second, law makers should create a binding alternative dispute resolution process so that courts are not inundated with lawsuits. An independent arbitrator system would be an ideal solution. The arbitrator would hear social networking disputes on the condition that the parties

109. *See* Neil Robinson et al., *Review of EU Data Protection Directive*, (Info. Comm'r's Office, Working Paper No. WR-607-ICO) (showing recent developments into data protection); C. Millard, *The Future of Privacy: Part 1—"Privacy 1.0": The Need for Change*, E-COMM DATA PROT. L. & POL'Y (2007) 4(11) (advocating for needed areas of improvement to data protection provisions).

110. *See* Council Directive 95/46, *supra* note 7, art. 6.1(a).

agree to be bound by decisions that are based on the applicable law.[111]

Third, Supervisory Authorities should take a proactive approach to raise awareness of the applicability of the data protection laws to social networking sites. If the goal is to effectively apply the data protection laws to social networking sites, it is important that SNS users and social networking providers understand the extent of regulation and applicability. Social networking providers should consider building in "privacy conscious" ways to protect a user's identity. Today, social networks are deploying sophisticated technological measures[112] for the user to configure their privacy settings,[113] but user etiquette remains largely unaddressed. Unfortunately, the seemingly simple solution of removal or deletion of the alleged contentious content opens other issues regarding freedom of speech and censorship.[114] A proactive step could be to implement a simple education on user etiquette, which would be enforced mostly through peer pressure, coupled with a limited reactive deletion strategy.[115]

While increasing responsibility of social networking providers, implementing effective alternative dispute resolution processes, and raising awareness regarding DPD laws and privacy issues would partially remedy a substantial component of the problem, these steps do not offer a complete solution. There is still much work to do in shaping data protection frameworks and laws to fit the needs of a fast- and ever-changing landscape.

VI. CONCLUSION

The growth of social networking websites have left the legal world in a game of "catch up." Those charged with the development of data protection schemes continue to evaluate and make recommendations. Educating the younger generation and the neophyte user about the wider availability of personal information and the potential liability attached to its misuse is a good starting point. However, the data protection framework also needs to be strengthened so that it is more robust with stronger remedies for misuse of an individual's personal information. This process has already begun with legislation being introduced by

111. Any applicable exemptions will be clearly and narrowly interpreted and applied.

112. *See* BROWN ET AL., *supra* note 3.

113. *Id.*

114. *See* Grimmelmann *supra* note 28.

115. *See generally* Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/information/ guide/index_e.cfm (discussing guidelines for data protection on social networking sites).

some Member States to strengthen the remedies and some Privacy Commissioners looking into the social networking issue.[116] The Article 29 Working Party's Opinion addressing social networking issues is certainly a step in the right direction. While the legal game of "catch-up" may never be completely won, the progress being made is encouraging and will continue.

As data protection authorities work through the problems, it is important that current data protection frameworks be applied in a reasonable fashion to social networking sites, and that SNS users' frustrations and concerns continue to be of importance in the decision-making process. Individual awareness, responsibility, and assistance through education will assist in abating the involuntary hijacking of private information. Users should be aware of the ongoing perils associated with using social networking sites so that social networking remains an enjoyable and useful activity while unauthorized impersonations of life become a welcome thing of the past.

116. *See, e.g.*, U.K. MINISTRY OF JUSTICE, CIVIL MONETARY PENALTIES: SETTING THE MAXIMUM PENALTY (2009), http://www.justice.gov.uk/consultations/docs/civil-monetary-penalties-consultation.pdf (discussing the UK Ministry of Justice's process of consultation to increase the penalties for data breaches); *see also* Hunton and Williams LLP Privacy and Information Security Law Blog, *U.K.'s Ministry of Justice Launches Consultation on Fines for Data Breaches*, http://www.huntonprivacyblog.com/2009/11/articles/european_union-1/uks-ministry-of-justice-launches-consultation-on-fines-for-data-breaches/. For information on Germany's recent introduction of new amendments to the Federal Data Protection Act 2001 see Hunton and Williams LLP Privacy and Information Security Law Blog, *Germany Adopts Stricter Data Protection Law – Serious Impact on Business Compliance*, http://www.huntonprivacyblog.com/2009/07/articles/european-union-1/germany-adopts-stricter-data-protection-law-serious-impact-on-business-compliance/ and Thomas Hoeren, *The New German Data Protection Act and its Compatibility with the European Data Protection Directive* 25(4) COMPUTER L. & SEC. REPORT 318 (2009).