Spring 2008

All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet, 25 J. Marshall J. Computer & Info. L. 241 (2008)

Rebecca Wong
Joseph Savirimuthu

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

http://repository.jmls.edu/jitpl/vol25/iss2/2

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
ALL OR NOTHING: THIS IS THE QUESTION?
THE APPLICATION OF ARTICLE 3(2)
DATA PROTECTION DIRECTIVE 95/46/EC TO THE INTERNET

REBECCA WONG† AND JOSEPH SAVIRIMUTHU††

I. INTRODUCTION

The exponential growth of social networking Web sites, online personal journals and the use of multimedia by individuals, raises important questions about the compatibility of Article 3(2) of the Data Protection Directive 95/46/EC ("DPD") as applied to the internet. The provisions in the DPD were designed to mediate between the rights of freedom of expression and privacy, however, it is not entirely clear whether the premises informing the scope of Article 3(2)† can be insisted upon in the light of the transformation taking place. Private individuals


1. Data Protection Directive 95/46, art. 3, 1995 O.J. (L 281) 31–50 (E.C.) (providing that the Directive will be inapplicable in two instances. The DPD excludes the processing of personal data taking place as part of activities falling outside of Community law. Also, the Directive is also deemed to be inapplicable if the processing of personal data is undertaken

241
can now assume a central role in the collection, processing, and distribution of data. Article 3(2) uses the European Court of Justice's ("ECJ") holding in *Lindqvist v. Jönköping*,\(^2\) as a framework for evaluating two key issues raised by the emergence of new social spaces for processing and disseminating information. First, it is not entirely clear from the emerging post-*Lindqvist* jurisprudence, whether the extension of Article 3(2) may necessarily undermine the fundamental principle of fairness and ultimately the coherence of the data protection legislation.\(^3\) The second issue is whether alternative regulatory instruments may enable the DPD to continue with its legal standard setting role. This article sets forth two conclusions dealing with these issues. The first conclusion is that it would be premature to extend the scope of Article 3(2). The second conclusion is that the future standard setting role of DPD must now embrace the emerging reality of a gradual convergence between systems of social interaction and systems of technological innovation.

II. *LINDQVIST*: BALANCING THE FREEDOM OF EXPRESSION AND RIGHTS OF PRIVACY

New communication technologies and the Internet compel us to assess whether an optimal balance is currently maintained between the rights of expression and privacy. The ECJ's ruling in *Lindqvist* provides an illustration of the factors that must be taken into account when seeking to find a balance between the rights of privacy and freedom of expression.

Before turning to the ECJ's ruling, it is pertinent to discuss some account of the regulatory framework governing the processing of personal data under the DPD. The purpose is not to undertake an exhaustive analysis of the jurisprudence on this subject\(^4\) but to highlight the rationale and organizing principles. The standard setting function of DPD cannot be properly understood without some familiarity with the organizing principles that assist the ECJ in balancing the competing claims made by litigants.

The DPD was passed in 1995 to harmonize the laws on data protection within the European Community. It required EU member states to


\(^{3}\) Data Protection Directive 95/46, art. 3, 1995 O.J. (L 281) 31-50 (E.C.) (stating the data protection legislation and what is principally referred to in the above text).

implement legislation by October 25, 1998.\(^5\) This DPD is further supplemented by the Directive on Privacy and Electronic Communications 2002/58/EC ("DPEC"), which applies to the processing of personal information carried out "in connection with the provision of publicly available electronic communications service in public communications networks in the Community."\(^6\) For the purposes of this article, only the latter half of Article 3(2) of the DPD will be considered. The following principles can be said to be key in the mediatory role of the DPD in balancing the competing interests between ‘data controllers’ and data subjects in respect of the processing of personal data. These principles are:

- Fairness
- Lawfulness
- Specificity
- Adequacy
- Accuracy
- Non-excessiveness
- Accessibility to the data subject.\(^7\)

These principles can be viewed as performing a standard setting function in the sense that the activities of ‘data controllers’ are now brought within a centralized regulatory framework designed to achieve transparency, accountability, and consistency in the application of the rules governing the collection, processing, and distribution of data. The obligations imposed by the DPD on ‘data controllers’ in specified circumstances can serve as an illustration of the standard setting process, in particular, the interplay of the principles of fairness and considerations of efficiency. For example, in relation to matters involving the processing of sensitive information relating to sex, health, and race, explicit consent must be obtained from the subject.\(^8\) This requirement is relaxed


\(^6\) See also Christopher Kuner, European Data Privacy Law: Corporate Compliance and Regulation (2d ed. 2007) (analyzing the application of the Directive on Privacy and Electronic Communications 2002/58/EC in the online environment).

\(^7\) See Data Protection Directive 95/46, art. 7, 1995 O.J. (L 281) (Article 7 provides six criteria in which personal data can be processed legitimately. These include the (1) data subject’s unambiguous consent (2) where this was necessary for the performance of a contract or at the request of the data subject prior to entering into a contract (3) compliance with a legal obligation.).

\(^8\) See also Privireal, Privacy in Research Ethics and Law, http://www.privireal.org/content/recommendations/#Rece (last visited Apr. 2007) (The DPD does not define what “explicit” consent is and there are different interpretations from EU Member States on
where the processing is seen as necessary to enable the 'data controller' to comply with obligations imposed by national laws or where the controller has legitimate interests in processing the data. The issues of explicit and implicit consent lie at the core of the standard setting role. The intention here is that 'data controllers' will assume a primary role in establishing self-regulation processes that mirror the goals of the DPD.

Article 3(2) of the DPD can also be seen to embrace the goals of legitimacy and efficiency. Legitimacy corresponds with the expectation of citizens that exercises of authority to conform with constitutional norms and principles. Efficiency is consonant with the idea that legitimate governance is alive to considerations of employing strategies that promote compliance. The enactment provides that the obligations relating to the processing of personal data are inapplicable in two specific circumstances. First, the processing of personal data is inapplicable in situations where the processing of that data falls outside the scope of Community law. Secondly, the data is inapplicable in situations where the person in the course of a purely personal or household activity, undertakes the processing of personal data. The decision to exempt these obligations can be approached from two specific levels. First, at a constitutional level, any encroachment into the private, social spaces would be seen as unjustified and contrary to prevailing social norms and values. Comparatively, at a regulatory level, it is not feasible for the state or its enforcement authorities to secure compliance with the obligations therefore, such obligations are inapplicable to the DPD. The ECJ gives a glimpse of such ideas in its deliberations in *Lindqvist*.9

In *Lindqvist*, the Plaintiff had uploaded a Web site containing details about members of a Parish Church. The Website also contained information about a specific member, who had injured her foot. Lindqvist did not obtain the consent of any of the individuals whose information appeared in the Web site before posting the information. Lindqvist also failed to inform the Swedish Data Inspection Board, the supervisory authority overseeing data protection, as to the publication of the sensitive information regarding the health of the members of the Parish on the Web site. In this case, the ECJ emphasized that the circumstances were within the scope of the exemption stipulated in Article 3(2). The court discussed that it may be seen as reasonable for individuals to discuss events surrounding the church in the setting of a living room, however, the public aspect of the publication of the events on the Internet, required the ECJ to sanction Lindqvist. According to the Court’s ruling,

---

the rights of privacy cannot be overridden by individuals, relying on the
defense of personal use and the freedom of expression as sufficient
cause.

Another way to read the Court's ruling in *Lindqvist*, requires that any future attempts by individuals to post information about people on a Web site, will not be allowed to treat their rights of expression as absolute, rather than discussing it as parts of a whole. However, at a policy level, the approach adopted by the ECJ, suggested that the public interest in preserving privacy should not be ignored in the age of new communication technologies. A final point in *Lindqvist*, show that the ECJ was not discussing that the content of the type published was prohibited, but merely that the people presented on Lindqvist's Web site had an expectation of privacy and the right to be consulted, along with the opportunity to determine the publication of such personal information. The ECJ held that:

Thus, it is, rather, at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases that a balance must be found between the rights and interests involved. Consequently, it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality. Whilst it is true that the protection of private life requires the application of effective sanctions against people processing personal data in ways inconsistent with Directive 95/46, such sanctions must always respect the principle of proportionality. That is so a fortiori since the scope of Directive 95/46 is very wide and the obligations of those who process personal data are many and significant. The answer to the sixth question must, therefore be that the provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the ECHR. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order (emphasis

10. Data Protection Directive 95/46, art. 9, 1995 O.J. (L 281) (stating that “member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of the artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression”).
The submissions made by the Swedish and the Netherlands’ government during the court proceedings in *Lindqvist*, discussed the view that Article 3(2) should not apply to instances involving the publication of personal information on the Internet and in Web sites.

The Swedish government contended that Article 3(2) did not exempt individuals who publish personal information to an indeterminate number of people on the Internet. Similarly, the Netherlands’ government took the same view, holding that exceptions provided under Article 3(2) do not apply in cases such as this, and the “creator of an Internet page brings [sic] the data placed on it to the knowledge of a generally indeterminate group of people.”

The question is whether Lindqvist was able to use the Swedish exemption as provided under Section 6 of the Personal Data Act 1998? The ECJ held that the exception must be:

interpreted as relating only to activities which are carried out in the course of private or family life of individuals. This is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people (emphasis added).

The ECJ’s decision clarifies the extent to which individuals may be able to benefit from Article 3(2), when placing personal information on the Internet, however, it raises several questions. If it is accepted that limiting access of an individual’s Web page to family members will be exempt from Article 3(2) DPD, such that the Data Protection Directive 95/46/EC does not apply, where does one draw the line for individuals whose web pages may extend beyond family members?

For example, Joe Blogs runs a personal Webpage highlighting environmental concerns and limits access to only a specific group of environmental activists. Would Article 3(2) DPD then apply on the basis that Joe was running his Web page for personal purposes? An analysis according to *Lindqvist*, would show that the burden would be on the Web page’s maker to show that the Webpage was intended to be used for private purposes and not personal purposes. The burden to show that this Web page was intended for private purposes is a harder threshold to

---

13. Id. at para. 32.
14. See also *Lagen gäller även för annan behandling av personuppgifter [Swedish Personal Data Act] (Personuppgiftslagen [SFS] 1998:204) (Swed.), available at http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf (discussing that Sec. 6 of the Swedish Personal Data Act is not applicable to “processing of personal data that a natural person performs in the course of activities of a purely private nature”).
15. This is a hypothetical example.
prove versus showing that it was used for personal purposes. Furthermore, it would be difficult to prove whether the author intended the Web page to be used for private purposes, therefore satisfying the threshold set forth by the Court.

The ECJ took a narrow approach to the interpretation of Article 3(2) as applied to the Internet, however the decision in Lindqvist draws a distinction between private and public access on the Internet. Article 3(2) of the DPD places a burden on individuals to limit access of their Web pages to a defined group before such individuals might benefit from the Article. However, when applied to blogs/podcasts (aside from the technological solutions that are available), this can be problematic for the courts in determining which Webpage should be accessible or not. Recital 12 states that the interpretation of Article 3(2) of the DPD, "[w]hereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses." Clearly, it appears that Article 3(2) should be construed narrowly in the light of the ECJ's decision in Lindqvist, but such a narrow interpretation raises certain questions.

III. IMPLICATIONS ARISING FROM LINDQVIST

In this section, we explore the main implications arising from the Lindqvist decision and the effect the decision had on several EU member states in their decision making policies towards data protection.

A. LEGISLATIVE DIFFERENCES BETWEEN MEMBER STATES' DATA PROTECTION LAWS TO THE IMPLEMENTATION OF ARTICLE 3.2 DPD TO THE INTERNET

Based on where an individual is located, there are likely to be differences in the interpretation and the application of Article 3(2) as implemented by member states' data protection laws. The salient features of the National Data Protection Laws are described in the following sections of this Essay.

1. The United Kingdom

The United Kingdom Data Protection Act 1998 ("DPA") replaces the 1984 Data Protection Act and implements the DPD. The DPA took effect on March 1, 2000. Currently, changes have been made to the DPA through the Freedom of Information Act of 2000 ("FIOA").16 These changes include the definition of 'data', and the change of the supervisory authority's name from the Data Protection Commissioner to the In-

Before discussing this issue further the definitions of ‘data’ and ‘personal data’ must be addressed. “Data” is defined under Section 1 of the DPA as information which:

- is being processed by means of equipment operating automatically in response to instruments given for that purpose,
- is recording with the intention that it should be processed by means of such equipment,
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
- does not fall within paragraphs (a), (b) or (c) but form part of an accessible record as defined by Section 68 of the DPA,
- is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

“Personal data” is defined under Section 1 of the DPA as:

Data which relate to a living individual who can be identified:

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual.

The definition of “personal data” has, however, been narrowly restricted in the recent Court of Appeal’s decision in *Durant v. Financial Services Authority*, which held that:

[N]ot all information retrieved from a computer search against an individual’s name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser

---

17. *Id.*
18. Accessible record is defined under Sec. 68 as education, health or accessible public record and was created under the DPA, but not found in the Data Protection Directive 95/46/EC.
19. Added following the FOIA.
20. The DPD places an emphasis on and discusses a ‘natural person’ as a living individual, but does not expressly provide for legal persons (ie: corporations, companies, etc.), hence the specific reference in terminology. There has been some academic discussion that focused on whether the DPD applies to deceased individuals, the idea being that even if they cannot make a request, then their estate would be permitted. However, this would be stretching the definition of a ‘natural person’. See Privireal, Recommendations, http://www.privireal.org/content/recommendations/#Recf, (last visited Mar. 18, 2008).
degree. It seems to me that there are two notions that may be of assistance. The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second one of focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated (emphasis added).  

Irrespective of the ECJ's recent Lindqvist decision, which interpreted "personal data" in light of the DPD, it is arguable that the mere mention of an individual on a Web page will not be sufficient to constitute "personal data" under the DPA. An essential factor in determining whether a Web page is 'personal data' is whether an individual's privacy has been compromised. This is balanced with other factors, such as, the freedom of expression as provided under Article 10 of the European Court of Human Rights ("ECHR").

There have been relatively few cases brought under the DPA regarding blogs and Web pages whereby individuals are prosecuted for placing personal other's personal information on Webpages, regardless of whether the site is accessible by the public. It is unclear why this is the case, in a recent correspondence with the United Kingdom Office of the Information Commissioner on the publication of personal information on the Internet, the following reply was given:

We have in the past received correspondence about data published on Web sites run by private individuals, such as amateur genealogy Web sites and personal home pages. Processing in these cases is often exempt from the DPA by virtue of the exemption of section 36. . . .There is, therefore, no action the Commissioner can take in response to such complaints.

Section 36 of the DPA provides that personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes), are exempt from the DPA. However, there are difficulties with reconciling Section 36 of the

24. Id.
DPA with the ECJ’s decision in Lindqvist. To recapitulate, the ECJ held in Lindqvist that:

The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) 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 (emphasis added).

Although, the ECJ dealt with the subject of processing personal data, there was clearly no question that the posted information was “personal information.” However, it is also difficult to reconcile the decision in Lindqvist with that in Durant.

The decision in Durant takes a practical approach to the interpretation of “personal data” so it excludes cases that are not clear cut, against individuals who make a passing reference to individuals on their Webpages. However, Durant does not detract from the idea that a person is still posting other people’s “personal data” on their Web site, as defined under the DPD. Article 2(a) of the DPD broadly defines “personal” as:

\[\text{Any information relating to an identified or identifiable natural person} \]

('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The Court of Appeal, in dealing with personal information, should have considered the exemptions provided under the DPA, rather than rule directly on whether the data was “personal”. Such exemptions under the DPA include: special purposes of processing for journalistic, artistic, and literary purposes Likewise, the Court of Appeal should have ruled as provided under Sections 27-39 of the DPA. By the Court of Appeal limiting the definition of the scope of “personal data”, the decision in Durant, not only has the difficulty of reconciling the decision in Lindqvist, but can be criticized that the DPA is weak by comparison to other Member States’ data protection laws.

25. Lindqvist, 1 C.M.L.R. 20.
26. Data Protection Act, 1998, c.29 §3 (U.K.). (defining “special purposes,” which are to be interpreted in light of Section 32 of the DPA, discussing journalism, literature, and art).
27. Id. at §27-39 (U.K.) (exempting the processing for purposes of national security (§ 28), crime and taxation (§ 29), health, education, and social work (§ 30), regulatory activity (§ 31), journalism, literature, and art (§ 32), research, history, and statistics (§ 33), and domestic purposes (§ 36).
2. Sweden

Sweden was the first country to have data protection laws. The Swedish Personal Data Act ("PDA") implements the DPD. Before looking at the relevant provision, this it is relevant to include a brief background of the PDA.

When the PDA was enacted, it was met with opposition from newspapers and the general public. According to Seipel, there were three main criticisms of the PDA. First, the PDA was considered a serious threat to the freedom of speech and civil liberties. However, the recent Ramsbro decision by the Swedish Supreme Court considered the exemptions provided under Article 9 (as implemented under the PDA 1998). In part, this decision addressed the question of processing for the purposes of "journalistic, artistic and literary purposes." This subject will be revisited in more detail, later in the article.

A second criticism of the PDA was that the DPD was outdated and that the Swedish legislators had to look for national solutions based on the regulation of misuse, rather than adopt an inclusive "processing model" as covered under the DPD. The changes to the PDA to adopt a misuse-orientated approach has now taken effect as of January 2007.

---

30. Id.
31. Id.
34. See Government Offices of Sweden, Data Protection, http://www.sweden.gov.se/sb/d/2771ljessionid=ATUP2PKsfaba (last visited April 2007) (explaining the background of the Swedish misuse-orientated approach); see also Government Offices of Sweden, Personal Data Protection: Information on the Personal Data Protection Act, http://www.sweden.gov.se/content/l/66/07/43/65/0ea2c0eb.pdf (last visited April 2007) (providing background of the Personal Data Protection Act); see also Josefine Johnson, Proposal to Amend the Swedish
Section 6 of the PDA provides that, "[t]his Act does not apply to such processing of personal data that a natural person performs in the course of activities of a purely private nature." This provision is likely to be interpreted in the same way as Lindqvist was. The misuse-orientated approach means that activities involving E-mail processing and Internet publishing, may be exempt from the PDA, if one can show that the PDA does not cause harm to the individual nor intrude their personal integrity.\textsuperscript{35} The PDA principally applies to processing that involves unstructured materials, such as running texts, sounds, and images. Materials that are structured to significantly facilitate searches for, or compilations of, personal data, such as personal data registers and personal data-related databases, would still fall within the scope of the PDA.

What begins to emerge as a result, is a two-staged test as provided under the PDA. This test requires one to first consider the application of the PDA under Section 6 in the light of Lindqvist. If Section 6 does not apply, one would then consider whether the misuse-orientated approach could exempt the activities (unstructured files) in question. Although such a two-staged approach would appear cumbersome, the Swedish Legislative Authorities bravely attempted to deal with the application of their data protection laws to the internet. This is particularly the case with the growth of blogs, podcasts, and Web 2.0. However, the adoption of the misuse-orientated approach only provides a short-term solution. Whether legislative change is adopted throughout Europe is less than clear.\textsuperscript{36}

3. Norway

Although Norway is not part of the European Union, but rather part of the European Economic Area, the country has enacted data protection laws since 1978. The first data protection law was the Data Registers Act.\textsuperscript{37} The present data protection law is the Norwegian Personal Data

\textsuperscript{35} See Lee A. Bygrave, \textit{Data Protection Law: Approaching its Rationale, Logic and Limits} 129 (2002) (claiming that "personal integrity is a question determined by the Swedish courts).

\textsuperscript{36} Oman, \textit{supra} note 29.

Act 2000 ("PDA 2000"), which took effect on January 1, 2001. Prior to the Lindqvist decision, individuals were not prosecuted for publishing personal information on the Internet if they could show that the Webpage was intended for private purposes. "Private purposes" were interpreted broadly to include a number of Websites that were set up for private purposes, such as an individual's hobby interests. However, the Norwegian Data Inspectorate is in the process of reviewing this provision. Professor Bygrave and Professor Schartum, two experts on the subject, have written a report recommending changes to the existing Norwegian data protection law. They propose to amend the PDA 2000 so that it is consistent with the Lindqvist decision. It is not clear whether the Norwegian Authorities will adopt this proposal, but already, the repercussions of the Lindqvist decision are noticeable.

4. Germany

The Federal Data Protection Act of 2001, or Bundesdatenschutzgesetz ("BDSG"), implements the DPD, and regulates the federal government agencies; private bodies; and state (Länder) data protection laws that apply to their own public bodies. The relevant provision under the FDPA 2001 provides:

The Act shall apply to the collection, processing and use of personal data by:

---

41. Grateful acknowledgments to Dr Jörg Hladjk, Hunton and Williams for his assistance.
44. See also Simitis, supra note 44.
Private bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection, processing or use of such data is effected solely for personal or family activities (emphasis added).

A restrictive interpretation is applied to fulfil the obligation of the Act under international law. For example, processing was shown to be used exclusively for private purposes, such as a personal electronic organizer. Furthermore, this provision will have to be construed in accordance with of the Lindquist decision. It is important to draw a distinction between processing for personal and professional purposes. What is personal depends on the general views of society at any given point in time. For instance, if used for private purposes, today's society views, addresses, phone numbers, web addresses, e-mail addresses, birthdays of colleagues, as well as other information regarding friends and relatives as personal. However, while the aforementioned examples would be private, the distinctions are not always clear when applied to the Internet. This is particularly true when the distinction is to be made with respect to the information available through social networking.

The German Telemedia Act of 2007 or Telemediengesetz ("TMG") has recently been enacted. The TMG replaces the Teleservices Data Protection Act, and the Federal Media Services Treaty. The TMG was enacted in March of 2007, and applies to electronic information, as well as, communication services, including Webpages, music download platforms, Internet search engines and E-mails. The TMG applies to most Web pages, but in Germany, independent of the Federal Data Protection Act 2001. In a presentation given by Dr. Weichert, head of the Centre for Data Protection in Schleswig-Holstein, the view was that the TMG did not apply to private homepages that were used for private and family purposes. However, there are problems differentiating between a Webpage created by an individual that is maintained for private purposes, and a Webpage that forms part of a social networking Website. On such example of this is registering on a Web site such as Myspace. As a result, there is no definitive answer to such a grey area. Differences

45. Id. Grateful acknowledgments to Dr Jörg Hladjk for his views.
46. Id.
47. Web 2.0 etc. is a topic which is explored later.
can be drawn between a Webpage solely maintained by an individual for private purposes, and Webpages that are formed as part of a social networking Website accessible to anybody, such a distinction can might be too simplistic when discussing the structure of the Internet.\textsuperscript{51}

The TMG utilizes definitions similar to those contained in the preceding law, the Teleservices Data Protection Act 1997\textsuperscript{52} ("TDDSG"), and regulates telemedia service providers.\textsuperscript{53} Although the TMG utilizes the same definitions as the TDDSG, for "contractual data" and "utilization data"\textsuperscript{54} there have been criticisms made against the TMG for not reaching as far as it had originally been anticipated. For example, VoIP is covered under the German Telecommunications Act 2004,\textsuperscript{55} but not under the TMG. However, video streaming is covered under the TMG.

In short, the TMG is unlikely to apply to private Webpages that are maintained by individuals. However, it is certain that more clarity is needed as to the TMG's application to Websites that are not managed by private individuals, but form part of social networking Web sites, such as MySpace. The main determinate in situations where this becomes an issue is who is the "data controller." By identifying who the data controller is, it will be easier to determine who is required to adhere to the relevant data protection laws before deciding whether social networking Web sites (MySpace; Facebook) fall outside the scope of the Data Protection. This may happen either through Article 3(2) DPD as implemented under the DPD or under the exemptions under Article 9 for special purposes, or Article 13 of DPD as implemented under corresponding data protection laws.

As set out in Article 1.1 of the DPD, \textit{imbalance exists in the protection of fundamental rights and freedoms of individuals} because the DPD

\textsuperscript{51} See also Jack Goldsmith & Tim Wu, Who Controls the Internet (2006); Laurence Lessig, Code and Other Laws of Cyberspace (1999); Andrew Murray, The Regulation of Cyberspace: Control in the Online Environment (2007).


\textsuperscript{53} See § 13 of the TMG (setting forth the duties of Telemedia Service Providers).


is favors the privacy\textsuperscript{56} of an individual moreso than information being posted on the Internet without their approval. Consequently, this leads to the encroachment of another's right to express without being subject to the data protection laws.\textsuperscript{57} If a literal interpretation of Article 3.2 is applied, then a consequence may be the Courts being overprotective of an individual's privacy, when such privacy is not being affected or misused. It is possible that that the protection of one's right to have his or her personal information protected is also a restriction on another person's right to express his or her views online and as a result, may become a consequence of such interpretation of Article 3.2 of the DPD. Article 1.1 of the DPD does not simply protect the privacy of an individual, but also the fundamental rights, and freedoms of individuals, including the freedom of expression.\textsuperscript{58}

B. WHAT IS CONSIDERED "PRIVATE" ON THE INTERNET?

The Lindqvist case redefines what is private on the internet. It has the undesirable effect of creating a public/private partition by placing an burden on individuals to limit access of their Webpages, if they want to be exempted from coverage under Article 3(2) of the DPD. Thus, it is arguable that the fostering of "social networking", through the use of such social networking Web site such as Facebook and MySpace, may be inhibited as a result of the Lindqvist decision. There exists further difficulty in determining the nexus group in which an individual may benefit. In other words, would an individual still be able to qualify under the exemption on the basis that his Webpage is accessible to those who are not family members? A narrow interpretation of Article 3(2) of the DPD would take the approach of limiting access of a Webpage to family members. On the other hand, a broader interpretation would include individuals, other than family members as those that would have limited access to the Web page. The lack of precedent in this area leaves this question open, but if one were to consider the legislators of the DPD's original intentions, then a limited interpretation would be used.


\textsuperscript{57} Article 9 of the Data Protection Directive 95/46/EC leaves it to the discretion of Member States to derogate, but the ECJ's ruling has left it to the national courts to decide.

\textsuperscript{58} See also Deryck Beyleveld, Overview of Directive 95/46/EC, http://www.privireal.org/content/dp/directivecommentary.php (last visited Feb. 15, 2008).
C. The Issue of “Personal Data”

The DPD takes a wider definition to “personal data”. Article 2(a) defines “personal data” as:

Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (emphasis added).

Recital 26 of the DPD further provides that:

[w]hereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

The wide definition of the DPD means that personal information of cursory reference is likely to fall within the realm of the DPD, which the ECJ’s Lindqvist decision also reflects.60

First, preliminary observations suggest that varying approaches to the scope of Article 3(2) indicate an ongoing assessment of the standard setting role of DPD. Second, the discussions about the remit of the DPD, and effective governance is particularly relevant to the present debate on the way information communication technologies shape expectations about the way individuals view the Internet, and issues relating to the management of their identity. Issues concerning technological innovation, and changing expectations of identity may render the seemingly standard, setting role under the DPD to appear inconsequential. The Essay will now briefly discuss social networking Websites to highlight their technological, and social significance, in order to properly address these Web sites’ potential impact on the DPD.

IV. SOCIAL NETWORKING SPACES

New technologies are now facilitating the creation of social spaces for interaction. The rise in media literacy, increased Internet penetration, and cheap broadband access has led to the growth of blogs, and

59. The UK’s definition of “personal data” in Durant v. FSA is not considered in this article.

Websites for user-generated content such as YouTube. Web sites such as Youtube show some of the ways that technological innovation and end-to-end architecture is converging with emerging social attitudes towards information, identity, and privacy. Information, or data resources can be used, recreated, and shared on such Web site. According to the Pew & Internet American Life Project, teenagers today are leveraging the interactive capabilities of the Internet to create, and share their own media creations. Many individuals now upload videos, photos, and digital images onto Websites. Furthermore, individuals are now comfortable with the idea of archiving their interests, or profiles online. Blogs (otherwise known as personal Web site) often contain reflections, thoughts, or observations on current affairs, lifestyles, or personal interests. Some authors also use blogs as communication spaces to meet other users with interests in sport, photography, food, entertainment, or fashion. These personal Websites also have podcasts that visitors download from the Web site. Other Websites allow individuals to upload, and share photos. Emerging social networking sites such as, take the idea of self expression one stage further than most personal Web sites. As the information on the site states:

Wallop is a new type of social networking site combined with a marketplace for buying and selling graphical effects called Wallop Mods for your profile. At Wallop we believe the next wave is all about self expression online similar to the ways we express ourselves in the real world by purchasing clothes, decorating a room or wearing jewelry. While Wallop is great for communicating with your friends, it is also a rich platform for Flash designers and content creators to develop Mods and make money doing it. We make it easy for you to design and create Mods that allow

---

62. See Amanda Lenhart & Mary Madden, Pew Internet & American Life Project, Teen Content Creators and Consumers (2005), http://www.pewinternet.org/pdfs/PIP_Teens_Content_Creation.pdf (last visited Apr. 25, 2007) (identifying that there was a large uptake in younger teens in creating content on the internet).
65. Podcasts are MP3 audio recordings of interests that Web site authors can make themselves.
people to express themselves.\textsuperscript{69}

Blogs are frequently used to debate cultural, religious, or political issues. Other blogs border on more intimate activities.\textsuperscript{70} In the legal academy, blogs have become a popular avenue through which ideas are exchanged, and disseminated. According to Technorati, the search engine blog directory, there are over 112.8 million blogs.\textsuperscript{71}

Another example of the way individuals use and manage information, is on social networking sites like Bebo, MySpace, and Lunarstorm.\textsuperscript{72} Blogs have evolved from being pure Online diaries into social networks. Consider for example, the social networking site Facebook.\textsuperscript{73} This site has search and browser facilities to enable an individual to find their friends, persons living in a particular area, or studying at a School, College, or University.\textsuperscript{74} Social networking sites have also begun to reflect commercial interests.\textsuperscript{75}

With the convergence of the multimedia, and communication platforms, “moblogs” (mobile phone blogs) have enabled mobile phone users to use the mobile network to capture videos, take photographs, and distribute text and media.\textsuperscript{76} As with blogs, moblogs frequently contain a biography of the author and a calendar record of when entries are made. Mobloggers post information to a moblog to communicate, and record experiences, thoughts, opinions, news, events, or keep a diary. Advances in the accessibility to, and quality of, media available allow users to post entries in various formats, i.e. text, digital photography, video, and/or sound files.

These sites underscore the growing acceptance of social networking sites as environments for having fun, social ecosystems for information sharing spaces, and opportunities to make connections with the wider community.

\begin{footnotesize}
\begin{enumerate}
\item Id.
\item Facebook Home Page, http://www.facebook.com/.
\item Id.
\end{enumerate}
\end{footnotesize}
Preliminary conclusions can be drawn from the foregoing brief examination of the way individuals access new technology, and use information in the marketplace of ideas. First, individuals have a range of new technologies for accessing media, and sharing information. Second, increased connectivity has also increased individual exposure, and immersion to information. Third, as individuals spend more time in the social spaces, we can detect a shift in cultural attitudes towards space, information, identity, and privacy. Strangely enough, the concept of privacy is shaped by the original idea behind the Internet, which is to create an environment for the free flow of information. One clear illustration of the way the Internet is fulfilling its role in this context, is the blurring of the space between public and private. For example, in the privacy of one’s home, one could publish personal or private information online through a Blackberry, mobile phone, or wireless laptop. The data or information transmitted using these devices, becomes a central part of the interactive process of creation, use, and distribution. Fourth, society's understanding, and expectations about the ready availability, and use of information is being gradually shaped by the new social ecosystem. In this respect, the terms of service policies often found in social networking sites represent a new form of negotiation taking place between data providers, data controllers, and data subjects.

So how does this account complement the constitutional/regulatory paradigm of fairness and efficiency? A preliminary consideration is that information is now readily accessible in the social ecosystem. The end-to-end architecture, the speed, and scale of the technological innovation have provided much of the impetus for the free flow of information, and content creation. Identity management and privacy considerations now compete with market expectations of choice, availability, and efficiency. These considerations emphasize the importance of refusing to isolate the DPD framework from the broader relational dynamics between the individual, and media. Some of the strategies being adopted reflect the embryonic negotiation process mediated by software code, contractual instrument, and ideas about property and are not being currently witnessed. Put another way, Article 3(2) issues are potentially being resolved through social network spaces. For example, individuals who subscribe to Web sites such as Bebo, are reminded that:

Whenever you voluntarily post personal information in public areas, like journals, webLogs, message boards, and forums, you should be aware that this information can be accessed by the public and can in turn be used by others to send you unsolicited communications. Please exercise discretion in deciding what information you disclose.77
Additionally, MySpace has an indexing system that classifies communities through groups. This means that if an individual wanted to join a "private group," according to Article 3(2) of the DPD, that person would first have to become a member, and login to MySpace. This person then has the ability to choose a group and apply to join such group. Upon approval, the new member of group would have access to personal information not visible to non-members of such group.

However, the above issues should not detract from the dangers of personal information being posted on the Internet. In a recent article dealing with the data protection issues raised by blogs, it was observed that:

Private facts are personal details about someone that have not been disclosed to the public. A person's sexual gender-preference, a sex-change operation, and a private romantic liaison could all be private facts. Once publicly disclosed by that person, however, they move into the public domain. The Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002/58/EC), Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Article 8 of the European Convention on Human Rights establish a Europe-wide set of legal principles for privacy protection which are enacted in all EU Member States and Council of Europe (CoE) Member States, respectively. The overall objective of the Directives is the protection of information privacy by Member States of the EU.

Bloggers, who post photos from Flickr onto their sites will be deemed to accept the privacy policies of their hosts or service providers. For example, Yahoo's privacy policy permits bloggers on their site to specify whether they want their photographs to be accessible to the public, selected individuals, or only themselves. However, Yahoo may use the photographs to target advertisements based on the metadata and notes associated with the photo that the blogger posts. Advertisers may have the ability, through the same information, to target the individuals that appear in the posted photograph, as well.

Social networking spaces provide an apt illustration of how policymakers, industry and society are forced to leverage the innovative and social potential of the Internet, and at the same time deal with regulatory implications for DPD. A brief summary will highlight the difficult policy questions and tradeoffs facing society.

---

78. An example of such a group on Myspace is the 'Smiles Group'. Myspace Homepage, http://groups.myspace.com/smiles (last visited Mar. 2008).
A. TRANSBORDER ISSUES

Article 25(1) of the Directive 95/45/EC requires organizations transferring personal data to countries outside the European Union to ensure an adequate level of protection for the rights and freedoms of those individuals whose personal data is transferred. Some blogs may have material other than texts on its site. These blogs may contain photos, videos, pictures, and audio (podcasts). Note that in some web sites which host these sites, subscribers must abide by US law rather than EU law.

According to the analysis in Lindqvist, the ECJ stated that the uploading of Webpages does not constitute the transfer of personal data under Article 25, because the Article was drafted when an issue involving Web pages might have not been foreseeable. This does not mean that one would not be “processing” personal data as covered under the DPD, but that Article 25 of the DPD would not apply according to the Lindqvist ruling:

Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs. Lindqvist’s position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them. If Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet. Accordingly, it must be concluded that Article 25 of Directive 95/46 is to be interpreted as meaning that operations such as those carried out by Mrs. Lindqvist do not as such constitute a transfer [of data] to a third country. It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country. The reply to the fifth question must therefore be that there is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby
making those data accessible to anyone who connects to the internet, including people in a third country (emphasis added).\footnote{Lindqvist, \textit{upra note}. 11, at paras. 68-71.}

B. \textbf{DOES THE TRANS-BORDER TRANSFER OF PERSONAL DATA FALL WITHIN THE PERMITTED DEROGATIONS?}

Two issues are of concern when dealing with personal data and a trans-border transfer. First, is the principle of fairness and second, is whether the safety mechanisms that national governments set in place for trans-border transfer of personal data are adequate. The UK's approach to this issue balances the requirements of fairness and efficiency by requiring data controllers to determine the appropriate levels of protection necessary to any particular circumstance. However, there still exists a conundrum. How do we monitor and ensure that adequate levels of protection are maintained? Can or should contractual mechanisms imposed by web site operators and Internet Service Providers be relied upon to displace the safeguards set in place under the DPA?

C. \textbf{BLOGS AS DATA PROCESSING SITES}

Given the ease with which information can now be processed and the avenues for dissemination, there are some important issues. Many have commented on the potential employment and intellectual property issues, defamatory and hate speech issues, and privacy.\footnote{See Daniel Solove, \textit{A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere}, 84 \textit{WASH. U. L.R.}, 1195 (2006); \textit{see also} L.B. Ribstein, \textit{From Bricks to Pajamas: The Law and Economics of Amateur Journalism}, 48 \textit{WM. & MARY L. REV.} 185 (2006); \textit{see also} S. Vine, \textit{Blogs, Blaughs and Legal Issues}, EBL 6(8) 7-9 (2004).}

The Internet protocols enable data to assume a viral characteristic and control over the integrity and authenticity of information cannot be underestimated. There is an emerging practice of "counter-Googling."\footnote{A. Hill, \textit{This Week We Want to Know All About...Counter-Googling}, \textit{Observer}, Feb. 11, 2007, http://technology.guardian.co.uk/print/0,,329712441-117802,00.html.}

Visitors to a blog now use the information from the blog to find additional information about persons or events:

If consumers put their entire life stories online, and you as a company candidly refer to this public information AND make them an offer they can't refuse, more sales may be on the way. And bloggers, savvy consumers by nature, will no doubt introduce a 'no unsolicited sales' seal, the moment they grow tired of COUNTER-GOOGLING, making it clear what’s off limits and what’s fair game.\footnote{Trendwatching.com. \textit{Counter-Gooeling} http://www.trendwatching.com/trends/2003/09/COUNTER-GOOGLING.html, (last accessed Apr. 27, 2007.).}

More importantly, can the DPD consider both web hosts and individuals who have blog or social networking sites data controllers who must...
be responsible for processing. The point here is that individuals, using blog or social networking sites for personal purposes are reliant on commercial intermediaries to deal with the technical functionality. In the light of the applicable principles of fairness that provides an overarching framework, it is arguable that the DPD will hold both sets of parties accountable.

D. Exemptions

1. Balancing rights of expression and rights of privacy

Article 9 of the DPD enables Member States to provide for “exemptions or derogations from the provision... where this was carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.”

The transposition of this provision by EU Member States has not been entirely consistent (as each Member State has transposed this provision differently), but the ECJ was clear to emphasize that personal data does not conflict with the freedom of expression. However, it may be difficult to balance the competing interests such as, rights of expression and rights of privacy in such cases. In Ramsbro, an individual posted details of bank officials on a web site. The purpose behind the web site was to alert individuals of unscrupulous banks and unethical network-capitalists. The Court described much of the material on the web site that contained personal information as having an insulting nature. The Swedish Supreme Court had to weigh the balance between the protection of an individual’s privacy and an individual’s freedom of expression and took into account, the jurisprudence of the European Court of Human Rights.

The Swedish Supreme Court held that:

The fact that electronic or other media published texts contain insulting or deprecating data or judgments does not mean that this takes away its character of journalistic purpose. On the contrary such a fact is to be looked upon as a normal ingredient within the scope of a critical societal debate. As the European Court of Human Rights has stated, the

85. Council Directive 95/46, Article 2, 2002 O.J. (L 201) (broadly defining a “data controller” as ‘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...’ and therefore, in the light of this definition, individuals could also be regarded as “data controllers” who process personal information); see eg. Lindquist.
87. Ramsbro B-293-00, June 2001 at p. 11.
freedom of information also includes the right to present such an expression and such opinions and thoughts which insult, shock or disturb. The limitation to “solely” journalistic purposes [as provided under the Personal Data Act 1998] alludes firstly to make clear that a processing of personal data, which takes place in the mass media and by journalists for other than journalistic purposes are outside the limitation. The processing by mass media of personal data, for instance for factoring, advertising or mapping of reader’s profiles, thus falls outside the limitation. Any support for an idea that the expression “solely” should be interpreted as meaning that it, independent of the fact that publishing has had journalistic purposes, should be possible, on the basis of the Act on Personal Data, to penalize an attack on someone else’s good name and reputation cannot be considered to exist.88

The question is how do we balance the freedom of expression and the right to privacy in the blog? For example:89

Stella, my eighties style yuppie witch of a team leader, has spun herself into a frenzy of hyperactivity. She has been working, in her own words, “like a bastard mad hard working bastard mega-bitch,” adding that as long as her friend Becky is away in China, she might as well immerse herself in work, “because what else is there?” I pondered this for a split-second, before she answered that it’s all about incentives. She’s made it her goal to take Becky sausage tasting on her return from foreign shores. She wants to prove to her that we can live the high life here in Preston just as well as any bunch of Beijing bankers.90

In this example, if no one can identify who the person is, then it is not likely to fall within the scope of the DPD. However, if individuals can be identified, then this situation would fall within the scope of the DPD, more specifically a wider definition under Article 2(a). The question is whether this would fall outside the scope Article 3(2) DPD. Applying a narrow interpretation, Article 3(2) is unlikely to apply. It may be arguable that individuals intend only private viewers of their web sites if they take steps such that the web page was not available to the public domain. If one were to apply the UK’s definition of personal data, then it is possible to contend that one did not intend to process personal data as defined by the UK Court of Appeal, because such data would have to be more than biographical information. However, as argued above, such a definition is unlikely to be found analogous to the Lindqvist decision.

88. Id.
90. Id.
V. CONCLUSION

A proper assessment of the scope of Article 3(2) and its standard setting function cannot be divorced from social and technological innovations encountered in the Internet. Social networking sites provide an apt example of the way the convergence of technological innovation and society's expectations is challenging orthodox understanding of privacy and the ability of regulatory institutions to regulate the activities of data controllers. From the perspective of individuals who subscribe to social networking sites, the issue of whether Article 3(2) should or should not be extended may appear to be inconsequential. The growth of blogs and podcasts raises potential challenges to the existing European data-protection framework and national data protection laws. The Lindqvist decision highlights the tension that exists in protecting the privacy of an individual on the one hand, and the freedom of expression of the other. If the data protection laws are to evolve in a coherent and principled manner, then a broader perspective of data governance must be adopted and one which integrates businesses and consumers into the regulatory process. Only when we recognize the paradox of new technology and the significance of the way society views privacy, will we then avoid specific dangers, such as those identified in the Bangemann Report. As a result, Article 3(2) needs to be re-thought and revised.

Currently, Europe leads the world in the protection of the fundamental rights and freedoms of individuals with regard to the processing of personal data. The application of new technology, however, affects highly sensitive areas such as those dealing with the images of individuals, their communication, their movements, and their behavior. With this in mind, it is quite possible that most Member States will react to these developments by adopting protection, including trans-frontier control of new technologies and services.