Forthcoming John Marshall Journal of Computer and Information Law 2007/8

All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet

By

Rebecca Wong[1] and Joseph Savirimuthu[2]

Abstract

The Data Protection Directive 95/46/EC (hereinafter the "Directive") was passed in 1995 to harmonise the national data protection laws within the European Community with the aim of protecting the fundamental rights and freedoms of individuals including their privacy as set out under Art. 1 of the Data Protection Directive. The rules governing the processing of personal data are deemed to be inapplicable in the two instances outlined by Art.3(2). Processing of personal data taking place as part of activities falling outside of Community law are excluded from the DPD. The Directive is also deemed to be inapplicable if the processing of personal data is undertaken by a natural person in the course of a purely personal or

[1]Rebecca Wong is Senior Lecturer in Law at Nottingham Law School, Nottingham Trent University with teaching and research interests in Tort, Intellectual property, Data Protection and Cyberlaw. Her main areas of specialism are in data protection and privacy. She holds an LLB (1998), MSc (2000), LLM (2001), PCHE (2004) and a PhD (University of Sheffield, 2007) in data protection. Her recent publications include *Privacy: charting its developments and prospects*, In: *Human Rights in the Digital Age,* 2005 and *Data Protection Online: Alternative approaches to sensitive data*, *Journal of Commercial Law and Technology,* 2007 *Demystifying clickstream data: a European/US perspective*, *Emory International Law Review*, 2007, 20(2), 563-590.

[2] Joseph Savirimuthu is Lecturer in Law at Liverpool Law School, University of Liverpool. Teaching and research areas include Internet Regulation and Governance, Child Net Safety and Information Security. He holds an LLB (1987), LLM in International Business Law (1988), Diploma in Legal Practice (1997), PGCE (2004) and Certificate in Internet Child Safety (2007). His recent publications include *P2P@softwar(e).com: Or the Art of Cyberspace 3.0* (2007), *DRMs, RFID and Disruptive Code: Architecture, Dystopia and Eunomics* (2006), *Reflections on the Google Print Library Project* (2006) and *'Open Source, Code and The Architecture: It's the Memes Stupid'* (2005)

household activity. It is the second part of Art. 3(2), which is examined in more detail. The ruling by the European Court of Justice in *Lindqvist* provides us with a fresh opportunity to re-examine whether the policy justifications for the exclusion under Art 3(2) continue to remain relevant in the light of widespread use of new technologies such as blogs, podcasts and web pages for processing and distributing information. Greater clarity regarding the implication of new communication technologies for DPD policy is necessary if the laws on data protection are to evolve in a coherent and principled manner.

Keywords: Data Protection Directive 95/46/EC; internet, private purposes, blogs, podcasts

I. Introduction

The exponential growth of social networking websites, online personal journals and the use of multimedia by individuals raises important questions about the compatibility of Art. 3(2) of the Data Protection 95/46/EC (hereinafter the "DPD") as applied to the internet. Whilst it is true that the provisions in the DPD were designed to mediate between the rights of the freedom to expression and privacy, it is not entirely clear whether the premises informing the scope of Article 3(2)[3] can be insisted upon in the light of the transformation taking place. Private individuals now assume a central role in the collection, processing and distribution of data. This article uses the ruling by the European Court of Justice in *Lindqvist*[4] 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

[3] Article 3(2) of the Data Protection Directive provides that the Directive is deemed to be inapplicable in two instances. Firstly, the processing of personal data taking place as part of activities falling outside of Community law are excluded from the DPD. Secondly, the Directive is also deemed to be inapplicable if the processing of personal data is undertaken by a natural person in the course of a purely personal or household activity. It is the second part of Art. 3(2), which is examined in more detail.

[4] C-101/01 [2004] 1 CMLR 20.

coherence of the data protection legislation.[5] Second, whether alternative regulatory instruments may enable the DPD to continue with its legal standard setting role. Two conclusions are reached in this paper. First, that it would be premature to extend the scope of Article 3(2). Second, 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 ruling in *Lindqvist* can be seen as providing an apt 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 ruling, some account of the regulatory framework governing the processing of personal data under the DPD may be pertinent. The aim here is not to undertake an exhaustive analysis of the jurisprudence of this subject[6] but to highlight the rationale and organising principles. The point here is that the standard setting function of DPD cannot be properly understood without some familiarity with the organising principles that assist the ECJ in balancing the competing claims made by litigants. The Data Protection Directive 95/46/EC (hereinafter "DPD") was passed in 1995 to harmonise the laws on data protection within the European Community. It required EU Member States to implement legislation by 25 October 1998.[7] This DPD is further supplemented by the

[5] By data protection legislation, we are principally referring to the Data Protection Directive 95/46/EC and the EU countries' implementation of the Data Protective Protection 95/46/EC.

[6] For an analysis of the data protection laws, *see* LEE A. BYGRAVE. DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS (London: Kluwer, 2002); CHRISTOPHER KUNER. EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS (Oxford: Oxford University Press, 2003); Rosemayr Jay & Angus Hamilton. *Data protection: law and practice*, 2nd ed (London: Sweet & Maxwell, 2003).

[7] On the transposition of the DPD by EU Member States, see PRIVIREAL. *Data Protection – by country* at http://www.privireal.org/ and DERYCK BEYLEVELD. (ET. AL.) IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE IN RELATION TO MEDICAL RESEARCH IN EUROPE (London: Ashgate, 2004); European Commission. *Status of*

Directive on Privacy and Electronic Communications 2002/58/EC (hereinafter "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' (Art. 3(1) DPD).[8] For the purposes of this paper, the authors will consider the latter half of Art. 3(2) of the Data Protection Directive 95/46/EC. The following principles[9] 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 are:

a. Fairness;
b. Lawfulness;
c. Specificity;
d. Adequacy
e. Accuracy
f. Non-excessiveness
g. Accessibility to the data subject

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

implementation of Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data (http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm), Last accessed 20 March 2007.

[8] For an analysis of the Directive on Privacy and Electronic Communications 2002/58/EC *see also* CHRISTOPHER KUNER. *EUROPEAN DATA PRIVACY LAW*: *CORPORATE COMPLIANCE AND REGULATION*, 2nd ed, (Oxford: Oxford University Press, 2007).

[9] See in particular Art. 7 on the data protection principles laid down under the European Data Protection Directive 95/46/EC. Art. 7 of the DPD provide six criterion in which personal data can be processed legitimately. These include the (a) data subject's unambiguous consent (b) where this was necessary for the performance of a contract or at the request of the data subject prior to entering into a contract (c) compliance with a legal obligation etc.

the subject.[10] This requirement is relaxed 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.

Art. 3(2) of the DPD can also be seen as embracing the goals of legitimacy and efficiency. The former corresponds with the expectation of citizens that exercises of authority conform with constitutional norms and principles. The latter 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, in situations where the processing of personal data falls outside the scope of Community law. Second, and particularly relevant to the present paper, is the exemption from the DPD obligations where a natural person in the course of a purely personal or household activity undertakes the processing of personal data. The decision to exempt the obligations can be approached from two 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. At a regulatory level, it is not feasible for the State or its enforcement authorities to secure compliance with the obligations. We can get a glimpse of these ideas in the deliberations of the ECJ in the leading case of *Lindqvist*.[11] The facts can be briefly recounted. L had uploaded a web page containing details about members of a Parish Church. The website also contained information about a member, who had injured her foot. L did not obtain the consent of

[10] The DPD does not define what "explicit" consent is and there are different interpretations from EU Member States on this. The German Federal Data Protection (BDSG) requires written consent before sensitive data can be processed. UK, however, does not require written consent to process sensitive data, so express consent (even given orally) will be sufficient, provided it is clear. See also PRIVIREAL: *Recommendations around "explicit consent"* (http://www.privireal.org/content/recommendations/#Rece), Last accessed April 2007.

[11] C-101/01 *Lindqvist* [2004] 1 CMLR 20.

the individuals before posting the information on the website. L also failed to inform the Swedish Data Inspection Board, as to the publication of the sensitive information regarding the health of the members of the Parish on the website. There is no doubt that the courts are well aware of the potential collision between Articles 8 and 10 of the ECHR. What is particularly interesting about the approach adopted by the ECJ is that there is no presumption of Article 3(2) applying in actions for breach of the Directive. As the ECJ makes clear, it will not be enough for an individual to lay claim to a defence of reasonableness or the fact that there is a "de minimis" rule as to what constitutes personal data or whether the processing is wholly or partly the product of an automated process. This much can be gleaned from emphasis placed by the court on whether the circumstances involving L were within the scope of the exemption stipulated in Article 3(2). Whilst it may be seen as reasonable for individuals to discuss events surrounding the parish church in the setting of a living room, the public aspect of the publication on the events on the Internet, was regarded by the ECJ as meriting sanction. To put it another way, the rights of privacy cannot be overridden by individuals relying on the defence of personal use and the freedom of expression[12] as sufficient cause. Another observation that can be made about the ECJ's approach is that any future attempts by individuals will not be permitted to treat their rights of expression as absolute. The converse here is that at a policy level, the approach adopted by the ECJ suggests that the public interest in preserving privacy should not be ignored in the age of new communication technologies. Finally, it should be noted that the ECJ was not saying that the content of the type published was prohibited, but only that the subjects identified on L's website deserved to have their wishes of privacy respected or at the least that they deserved the right to be consulted and the opportunity to determine the publication of the 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*

[12] Freedom of expression is covered under Art. 9 of the DPD, which provides 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.'

> *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 added).[13]

In submissions made by the Swedish and the Netherlands Government during the Court Proceedings in *Lindqvist,* they took the view that Art. 3(2) should not apply to instances involving the publication of personal information on the internet.

The Swedish Government contended that Art. 3(2) did not exempt individuals who publish personal information to an indeterminate number of people on the internet.[14] Similarly, the Netherlands Government took the same view holding that exceptions provided under Art. 3(2) did not apply and that the 'creator of an internet page brings [sic] the data placed on it to the knowledge of a generally indeterminate group of people.'[15]

The question is whether *Lindqvist* was able to use the Swedish exemption as provided under s 6 of the Personal Data Act 1998?[16]

---

[13] *Lindqvist*, *supra,* note 11, at paras. 85-90.

[14] C-101/01, para. 31.

[15] *Id.*. at para. 32.

[16] s 6 of the Swedish Personal Data Act 1998 provides that the PDA is not applicable to 'processing of personal data that a natural person performs in the

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, which 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).'

Whilst the ECJ decision clarifies the extent to which individuals may be able to benefit from Art. 3(2), when placing personal information on the internet, it however, raises several questions. If it is accepted that limiting access of an individual's webpage to family members will be exempt from Art. 3(2) DPD such that the Data Protection Directive 95/46/EC does not apply, where does one draw the line for individuals whose webpages may extend beyond family members? For example, Joe Blogs runs a personal webpage highlighting environmental concerns[17] and limits access to a group of environmental activists? Would Art. 3(2) DPD then apply on the basis that Joe was running his webpage for personal purposes? From the analysis of *Lindqvist*, the onus would be on the individual to show that the webpage was intended to be used for private purposes, which appears to be a harder threshold to prove.

Although it could be argued that the ECJ took a narrow approach to the interpretation of Art. 3(2) as applied to the internet, the implications of this decision are that a distinction is drawn between private and public access on the internet. Art. 3(2) of the DPD places an onus on individuals to limit access of their webpages to a defined group before they could benefit and this can be problematic, when applied to blogs/podcasts (aside from the technological solutions that are available).

Recital 12 further assists with the interpretation of Art. 3(2) of the DPD:

> Whereas 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…

course of activities of a purely private nature.' See also the Swedish Personal Data Act 1998 at http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf.

[17] This is a hypothetical example.

Clearly, it appears that Art. 3(2) is to 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 *Lindqvist* decision and the effect of the decision it has 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 Art. 3.2 DPD to the internet. Based on where the individual is located, there are likely to be differences in the interpretation and the application of Art. 3(2) as implemented by Member States data protection laws. The salient features of the national data protection laws are described as follows:

A1 UK

The UK Data Protection Act 1998 replaces the 1984 Data Protection Act and was passed to implement the DPD. It took effect on 1 March 2000. To date, changes have been made to the UK DPA 1998 through the FOIA 2000 including the definition of data and the change of the supervisory authority's name. A few preliminary points concerning the definitions of "data" and "personal data". Data is defined under s 1 DPA 1998 as 'information which:

> (a) is being processed by means of equipment operating automatically in response to instruments given for that purpose,
>
> (b) is recording with the intention that it should be processed by means of such equipment,
>
> (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraphs (a), (b) or (c) but form part of an accessible record as defined by s 68,[18]

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).[19]

Personal data is defined under s 1 of the DPA as:

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

(a) from those data; or

(b) 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, *Durant v FSA*,[20] which held that:

> …not 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 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*

[18] Accessible record is defined under s 68 as education, health or accessible public record and was created under the DPA 1998, but not found in the Data Protection Directive 95/46/EC.

[19] Added following the FOI Act 2000.

[20] [2003] EWCA Civ 1746.

> *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).

Leaving aside the discussion over whether the interpretation of "personal data"[21] was correct in the light of the DPD and the recent decision by the ECJ in *Lindqvist's*, it can be seen that the mere mention of an individual on a webpage will not be sufficient to constitute "personal data" under the UK Data Protection Act. What will be a determining factor is whether an individual's privacy has been compromised and this will have to be balanced with other factors such as the freedom of expression as provided under Art. 10 of the ECHR.

On the discussion of blogs and webpages, there have been relatively few cases being brought under the UK DPA 1998, whereby individuals have been prosecuted for placing personal information of other individuals on their webpages (whether accessible by the public on the internet or not). Although it is unclear why this is the case, in a recent correspondence with the UK 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 websites run by private individuals, such as amateur genealogy websites 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.[22]

[21] In the context of "personal data", see also Watts, M. "Information, data and personal data - reflections on Durant v. Financial Services Authority" (2006) *CLSR* 22(4), 320-325; EDWARDS, L. *TAKING THE "PERSONAL" OUT OF PERSONAL DATA: DURANT V FSA AND ITS IMPACT ON THE LEGAL REGULATION OF CCTV*, (2004) 1:2 *SCRIPT-ED* 341, @: <http://www.law.ed.ac.uk/ahrc/script-ed/issue2/durant.asp>.

[22] Personal correspondence with the UK Information Commissioner's Office on 26th April 2006.

s 36 of the UK Data Protection Act 1998 (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.[23] However, there are difficulties with reconciling s 36 of the 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).[24]

Although the ECJ dealt with the subject of processing personal data, clearly, there was no question that one was dealing with personal information. It is difficult to reconcile the decision in *Lindqvist* with *Durant*. Whilst *Durant* seems to take a practical approach to the interpretation of "personal data" so that it has the effect of excluding trivial cases being brought before the national courts against individuals who may make a cursory or passing reference of other individuals on their webpages, it does not detract from the line of thought that one is still dealing with "personal data" as defined under the DPD, if one is referring to individuals on the webpage. Personal data is defined broadly under Art. 2(a) of the DPD 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.'

In dealing with personal information, it would have been preferable for the Court of Appeal to consider the exemptions provided under the UK DPA 1998 (such as special purposes (processing for

[23] As confirmed through written correspondence with the UK Office of the Information Commissioner.

[24] *Lindqvist, supra,* note, 11., at para. 19.

journalistic, artistic and literary purposes)[25] or as provided under ss 27-29 of the DPA[26] rather than rule directly whether the data was "personal". In limiting the definition of the scope of "personal data", the Court of Appeal's decision in *Durant* not only has the difficulty of reconciling the decision with *Lindqvist* (in particular, Art. 8 of the DPD, whereby the ECJ interpreted Art. 8 widely such that mere mention of someone's foot was sufficient to constitute the "processing" of personal data), but arguably opens itself to the criticism that the UK Data Protection is weak by comparison to other Member State[27] data protection laws that have implemented the Data Protection Directive 95/46/EC. Limited space does not permit the authors to explore the scope of "personal data" in any detail, but suffice it to state that the Court of Appeal's decision in Durant is not satisfactory.

A2 SWEDEN

[25] s 3 DPA 1998 defines "special purposes" which is to be interpreted in the light of s 32 of the DPA 1998, journalism, literature and art.

[26] In the UK, the exemptions are covered under ss 27-39 of the DPA 1998. These include processing for the purposes of national security (s 28 DPA 1998); crime and taxation (s 29 DPA 1998); health, education and social work (s 30 DPA 1998); regulatory activity (s 31 DPA 1998); journalism, literature and art (s 32 DPA 1998); research, history and statistics (s 33 DPA 1998); domestic purposes (s 36 DPA 1998).

[27] See for example, Iceland's Supreme court's decision in *Ragnhildur Guðmundsdóttir v the State of Iceland* 151/2003 (also available at http://www.epic.org/privacy/genetic/iceland_decision.pdf) and RENATE GERTZ, R. "AN ANALYSIS OF THE ICELANDIC SUPREME COURT JUDGEMENT ON THE HEALTH SECTOR DATABASE ACT", (2004) 1:2 *SCRIPT-ed* 241, @: <http://www.law.ed.ac.uk/ahrc/script-ed/issue2/iceland.asp>.

Sweden was the first country to have data protection laws.[28] The Swedish Personal Data Act ("PDA" hereinafter) implements the European Data Protection Directive 95/46/EC.[29] Before looking at the relevant provision, a few points to be made about the background into the Swedish Data Protection Act,[30] When the PDA was enacted, it was met with opposition from newspapers and the general public. According to Seipel,[31] there were three main criticisms levelled at the Act. Firstly, it was critiqued for being a serious threat to the freedom of speech and civil liberties. Indeed, the opposition was so tremendous that academics such as Professor Jacob Palme[32] became involved in the debate. However, the recent *Ramsbro*[33] decision by the Swedish Supreme Court that considered the exemptions provided under Art. 9 (as implemented under the Swedish Personal Data Act 1998) do, in part, address the question of processing for the purposes of "journalistic, artistic and literary purposes." We will consider this subject in more detail later in this article. A second criticism 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.

[28] For a background into the Swedish developments on data protection, see Peter Seipel. "Sweden" In: Peter Blume. *Nordic Data Protection Law*, 2001, pp. 123-151; See Őman, S. *Implementing data protection law* In: Wahlgren, P. IT Law, *Scandinavian Studies in Law*, 2004, 47, p.391; Mathias Klang, "Technology, Speech, Law & Ignorance – The state of free speech in Sweden", *Hertfordshire Law Journal*, 1(2), 48-63 (Autumn 2003); DAVID H. FLAHERTY, *PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA AND THE US* (University of North Carolina Press, 1989); Rebecca Wong, *The shape of things to come: Swedish developments on the protection of privacy*. *SCRIPT-ED,* 2(2) 107-124 @: http://www.law.ed.ac.uk/ahrc/script-ed/vol2-1/wong.asp (2005).

[29] *Id.*.

[30] *Id.*.

[31] Peter Seipel. *Supra,* note. 28.

[32] Jacob Palme . *Critical Review of the Swedish Data Act* (http://people.dsv.su.se/~jpalme/society/data-act-analysis.html), Last accessed April 2007 and *Freedom of Speech, the EU Data Protection Directive and the Swedish Personal Data Act* (http://people.dsv.su.se/~jpalme/society/eu-data-directive-freedom.html), Last accessed April 2007.

[33] B-293-00, June 2001.

The changes to the PDA to adopt a misuse-orientated approach has now taken effect from January 2007.[34, 35]

s 6 of the PDA 1998 provides that:

> This 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 light of *Lindqvist*." These changes took effect in January 2007.[36] The misuse-orientated approach means that activities involving e-mail processing and internet publishing may be exempt from the PDA 1998, if it can be shown that it does not cause harm to the individual or more specifically, intrusion into their personal integrity.[37] It principally applies to processing involving unstructured materials, such as running texts, sounds and images. Materials which are structured in order 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 Personal Data Act 1998.

What begins to emerge is a two-staged test as provided under the PDA 1998, whereby one would first consider the application of the PDA 1998 under s 6 (in the light of *Lindqvist*). If s 6 does not apply

---

[34] For a background into the Swedish Misuse-Orientated Approach, *see* Ministry of Justice. *Data Protection* (http://www.sweden.gov.se/sb/d/2771;jsessionid=aTUP2FKsfaba), Last accessed April 2007 and Swedish Personal Data Protection Act (http://www.sweden.gov.se/content/1/c6/07/43/65/0ea2c0eb.pdf), Last accessed April 2007 and Bird and Bird. *Proposal to amend the Swedish Personal Data Act – the first steps towards a misuse-orientated legislation* (http://www.twobirds.com/english/publications/articles/Swedish_Personal_Data_Act.cfm), Dated 22 March 2006 and Wong, R, *op. cit*. n. 28.

[35] The reference for the then bill is Prop 2005/06:173. Grateful acknowledgment to Mr Sören Öman for this reference. This can be found at http://www.regeringen.se/content/1/c6/06/08/09/2c0a24ce.pdf.

[36] *Id.*.

[37] "Personal integrity" is a question to be determined by the Swedish Courts. For a brief analysis, see also LEE A. BYGRAVE. *DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS*, 2002, p. 129.

to internet activities, then one would then consider whether the activities (unstructured files) in question can be exempt from the misuse-orientated approach. Although such a two-staged approach would appear cumbersome, it is a brave attempt by the Swedish Legislative Authorities to deal with the application of their data protection laws to the internet and this is particularly the case with the growth of blogs, podcasts and Web 2.0. The adoption of a misuse-orientated approach is, but a short-term solution. Whether change can be made at a European level is less clear.[38]

A3 NORWAY

Although Norway is not part of the European Union (but part of the EEA), it has enacted data protection laws since 1978 with the first one being the Data Registers Act.[39] The present data protection law is the Norwegian Personal Data Act 2000 (hereinafter "PDA"), which took effect on 1 January 2001.[40] Prior to the *Lindqvist* decision, individuals were not prosecuted for publishing personal information on the internet if it can be shown that this was intended for private purposes.[41] Private purposes were interpreted to include a number of websites which were set up for private purposes such as a hobby. However, this provision is in the process of being reviewed. Two experts, Professor Bygrave and Professor Schartum have written a report[42] recommending changes to the existing Norwegian data

[38] *Supra, note*. 34.

[39] For background reading into the Norwegian data protection law, see LEE A. BYGRAVE. *DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS*, 2002; LEE A. BYGRAVE & A.H. AARó. "NORWAY" IN: M. HENRY (ED) *INTERNATIONAL PRIVACY, PUBLICITY AND PERSONALITY LAWS* (London: Butterworths, 2000), pp. 333-346 and PRIVIREAL. Norway (http://www.privireal.org/content/dp/norway.php), Last accessed March 2007.

[40] See Norwegian Data Inspectorate. *Personal Data Act 2000* (http://www.datatilsynet.no/templates/Page____194.aspx), Last accessed March 2007.

[41] See Dag W. Schartum. "Norway" In: PETER BLUME (ED.) NORDIC DATA PROTECTION, 2001, p. 104.

[42] The report is in Norwegian. (http://www.personvern.uio.no/pvpn/artikler/utredning_personopplysningsloven.pdf), Last accessed March 2007.

protection law. One of the proposals is to amend the PDA so that is it in line with the *Lindqvist* decision. It is not clear whether these recommendations will be taken up, but already, the repercussions of the *Lindqvist* decision can be felt.

A4 GERMANY[43]

The Federal Data Protection Act 2001 (*Bundesdatenschutzgesetz*[44]) implements the DPD and regulates *federal* government agencies and private bodies and State (Länder) data protection laws[45] apply to their own public bodies. The relevant provision under the FDPA 2001[46] is § 1, paragraph 3 which provides that:

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

> 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).

---

[43] Grateful acknowledgments to Dr Jőrg Hladjk, Hunton and Williams for his assistance.

[44] Abbreviated "BDSG". For a commentary into the German Data Protection Laws, *see* Simitis, S, *Bundesdatenschutzgesetz*, 6th Rev Ed, Baden-Baden, Nomos 2006; HERBERT BURKERT. *Privacy/Data Protection: A German/European Perspective* (http://www.mpp-rdg.mpg.de/pdf_dat/burkert.pdf), Last accessed April 2007; Flaherty, D. H. *Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada and the US*, London: University of North Carolina Press, 1989. The English translation of the Federal Data Protection Act (as of 15 November 2006) can be found at:http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf.

[45] For a list of Länder data protection laws, this can be found at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm#germany, Last accessed April 2007.

[46] *See also* Spiros Simitis, *supra.*, note. 47.

A restrictive interpretation is applied to fulfil its obligations under international law.[47] For example, processing was shown to be used exclusively for private purposes such as a personal electronic organiser. Furthermore, this provision would have to be construed in the light of *Lindqvist*. An important distinction to be drawn is processing for personal and professional purposes. What is personal would depend on the general views of the society at the time.[48] For instance, addresses, phone numbers, web addresses, e-mail addresses, birthdays of colleagues, other information regarding friends, relatives and so forth would all be regarded as personal if used for private purposes. However, whilst it would be private, the distinctions are not always clear-cut when applied to the internet and this is particularly the case when we enter the realms of social networking (Web 2.0 etc.), a topic which is explored later.

Secondly, the German Telemedia Act 2007 (*Telemediengesetz*)[49] has recently been enacted, replacing the Teleservices Data Protection Act and the Federal Media Services Treaty.[50] This came into force on March 2007 and applies to electronic information and communication services including web pages, music download platforms, internet search engines and emails. The Act ("TMG" hereinafter) only applies to Germany and the effect of which (independent of the Federal Data Protection Act 2001) would generally apply to most webpages. In a presentation given by Dr Weichert,[51] Head of the Centre for Data Protection in Schleswig-Holstein, the view was that the Telemedia Act did not apply to private homepages (used for private and family purposes).

---

[47] *Id.*. Grateful acknowledgments to Dr Jőrg Hladjk for his views.

[48] *Id.*.

[49] *Telemediengesetz* (http://bundesrecht.juris.de/tmg/index.html), Last accessed May 2007. See Bygrave, L. A. *Data protection law: approaching its rationale, logic and limits*, 2002, pp. 328-329.

[50] *German Telemedia Act introduces new rules for new media* (http://www.twobirds.com/english/publications/articles/German_Tele_Media_Act_new_rules.cfm), Dated 5 March 2007.

[51] *Das neue Telemediengesetz – TMG* (https://www.datenschutzzentrum.de/vortraege/20070423-weichert-tmg.pdf), Dated 23 April 2007.

Notwithstanding this, there are problems in differentiating a webpage created by an individual maintained for private purposes and a webpage that formed part of a social networking website (for instance, registering on MySpace). There is no definitive answer to this grey area. Whilst differences could be drawn between a webpage solely maintained by an individual (for private purposes) and webpages that formed part of a social networking website, and accessible to anybody such a distinction can, arguably, be taken to be simplistic of the structure of the internet.[52]

The TMG draws also draws on definitions similar to the preceding law, the Teleservices Data Protection Act 1997[53] (hereinafter "TDDSG") and regulates Telemedia services providers.[54] Although the TMG retains the same definitions from the Teleservices Data Protection Act (application to "contractual data" (§ 14) and "utilisation data" (§ 15))[55] there have been criticisms made against the TMG for not going as far as anticipated. For example, VoIP is covered under the German Telecommunications Act 2004,[56] but not

[52] For a discussion about the internet, see also Laurence Lessig, CODE AND OTHER LAWS OF CYBERSPACE, 1999 (also available at http://code-is-law.org/); Andrew Murray. THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT, Oxford, 2007 and JACK GOLDSMITH & TIM WU. WHO CONTROLS THE INTERNET? Oxford, 2006.

[53] The English translation to the Teleservices Data Protection Act 1997 is available at http://www.iuscomp.org/gla/statutes/TDDSG.htm (but does not include the 2001 amendments – English translation is not available). However, the German version is available at http://www.artikel5.de/gesetze/tddsg.html (includes the 2001 amendments). For a brief background into the Teleservices Data Protection Act 1997, see Bygrave, L.A. "German Teleservices Data Protection Act" (1998) *Privacy Law and Policy Reporter*, Vol 5, pp. 53-54 at http://folk.uio.no/lee/oldpage/articles/Germany_TDPA.pdf.

[54] *See* § 13 of the TMG, which sets out duties of Telemedia Service Providers.

[55] *See* Lee A. Bygrave. *Supra*, note 52.

[56] See Telecommunications Act 2004 (TKG) at http://www.bfdi.bund.de/cln_030/nn_946430/EN/DataProtectionActs/Artikel/TelecommunicationsAct-TKG,templateId=raw,property=publicationFile.pdf/TelecommunicationsAct-TKG.pdf.

so under the new TMG, whereas video streaming would, however, be covered under the TMG. In short, the TMG is unlikely to apply to private webpages as maintained by individuals, but certainly, more clarity is needed when considering its application to websites that are not managed by private individuals but form part of social networking website such as MySpace etc. The key question to be asked is who is the "data controller". By identifying who the data controller is, then it would be easier to determine who is required to adhere to the relevant data protection laws, before deciding whether this falls outside the scope of the Data Protection (either through Art. 3(2) DPD as implemented under the DPD or under the exemptions under Art. 9 for special purposes or Art. 13 of DPD as implemented under corresponding data protection laws).

B. Imbalance that exists in the protection of fundamental rights and freedoms of individuals as set out in Art. 1.1 of the DPD such that the DPD appears to be heavily tilted towards the "protection of privacy" of an individual. Thus, leading to the encroachment of another's right to express without being subject to the data protection laws (Art. 9 leaves it to the discretion of Member States to derogate, but the ECJ's ruling has left it to the national courts to decide) If the literal interpretation of Art. 3.2 is applied, then it can have the consequence of being o*verprotective* of an individual's privacy when really his/her privacy is not being affected or misused. What is being argued here is 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. Art. 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 to expression.[57]

C. Question about what is "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 onus on individuals to limit access of their webpages, if they wanted to be exempted from Art. 3(2) of the DPD or corresponding data protection laws. Thus, it is arguable that the fostering of "social networking" and the communications between other individuals may

[57] See also Deryck Beyleveld. *Overview of Directive 95/46/EC* (http://www.privireal.org/content/dp/directivecommentary.php), Last accessed March 2007.

be inhibited as a result of the *Lindqvist* decision. There is a further difficulty with 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 reaches to those who are not necessarily family members? A narrow interpretation of Art. 3(2) of the DPD would take the approach of limiting access to a webpage to family members, but a broader view would include individuals other than family members. The scarcity of caselaw/precedent leaves this question open, but if one were to conform with the legislators' original intentions, when the DPD was passed, then a limited interpretation would be preferred.

D. Anomaly of the Lindqvist decision because the ECJ took the view that the uploading of webpages does not constitute a transfer of personal data to third countries under Art. 25 of the DD. The ECJ was prepared**,** however, to construe Art. 3.2 narrowly. We will discuss transborder data flows in section 4.1 of this paper.

E. The issue of "Personal Data": The Data Protection Directive 95/46/EC takes a wider definition to "personal data". Art. 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 'whereas 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.'

As discussed above, the wide definition[58] means that personal information of cursory reference is likely to fall within the realm of

[58] The UK's definition of "personal data" in *Durant v FSA* is not considered in this article.

the Data Protection Directive 95/46/EC, which is also reflected in the ECJ's decision in *Lindqvist*.[59]

We can make some preliminary observations. First, 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 are shaping our expectations about the way individuals view the Internet and issues relating to the management of their identity. To be sure, issues concerning technological innovation and changing expectations of identity may render the seeming standard setting role under the DPD to appear inconsequential. We can now turn to a brief discussion of social networking spaces to highlight their technological and social significance so that their potential impact for DPD can be properly addressed.

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 have led to the growth of blogs, and websites for user-generated content like You-Tube. The evolving social ecosystem shows some of the ways technological innovation and end-to-end architecture is converging with emerging social attitudes towards information, identity and privacy. Information or data now becomes a resource to be used, recreated and shared. 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.[60] 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.[61] It is common to find

[59] See also Douwe Korff. *Supra*, note. 88 – discussion of personal data as implemented by EU Member States.

[60] See http://www.pewinternet.org/pdfs/PIP_Teens_Content_Creation.pdf (accessed 25th April, 2007).

[61] See M Young, "Blogging: An Introductory Look at an Old Pastime in a New Medium" (2006) 23 Library Hi Tech News 27 - 28

blogs, which contain reflections, thoughts or observations on current affairs, lifestyle or personal interests.[62] The contents as well as the quality of the blogs will vary depending on its authors.[63] Some authors use blogs as communication spaces to meet other users with interests in sport, photography, food, entertainment or fashion. Some personal websites or blogs have podcasts which visitors to the site can download. Podcasts are MP3 audio recordings of interests. Some sites have photographs. Flickr, which has been recently acquired by Yahoo, enables individuals to share photos.[64] Emerging social networking sites like Wallop taking the idea of self expression one stage further.[65] As the information on the site states:[66]

> 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 people to express themselves![67]

---

http://callcentrediary.blogspot.com/ (a personal diary of a team manager at a call center)

[62] Wikipedia Blog at http://en.wikipedia.org/wiki/Blog (accessed February 15, 2007).

[63] See generally R Wray, How one year's digital output would fill 161bn iPods," Tuesday March 6, 2007 http://technology.guardian.co.uk/news/story/0,,2027327,00.html

[64] Flickr (http://www.flickr.com/), Last accessed April 2007.

[65] Wallop (http://www.wallopcorp.com/), Last accessed April 2007 and SubTV (www.SUB.tv), Last accessed April 2007.

[66] *Wallop Modder Network* (http://designer.wallop.com/), Last accessed April 2007.

[67] *Id.*.

Blogs are frequently used to debate cultural, religious or political issues. Others tend to be verging on more intimate activities.[68] 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 69 million blogs.[69] Another example of the way individuals use and manage information is that of social networking sites like Bebo, MySpace, Lunarstorm.[70] Blogs have evolved from being pure online diaries into social networks. Consider for example the social networking site Facebook.[71] This site has search and browser facilities to enable an individual to find their friends or persons living in a particular area or studying at School, College, or University.[72] Social networking sites have also begun to reflect commercial interests.[73]

With the convergence of the multimedia and communication platforms, "moblogs" have enabled mobile phone users to use the mobile network to capture videos, take photographs and distributing text and media.[74] As with blogs, moblogs frequently contain a biography of the author and a calendar to record when entries are made. Mobloggers post information to a moblog to communicate and record experiences, thoughts, opinions, news, events, or keep a diary.

---

[68] *Belle de Jour* (http://belledejour-uk.blogspot.com/) (a diary of a call girl in London), Last accessed April 2007.

[69] *Technorati* (http://technorati.com/about/) (accessed February 20, 2007)

[70] Pew & Internet American Life Report, *Teen, Privacy & Online Social Networks (April 2007), available at http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf (accessed on 25th April 2007).*

[71] *Facebook* (http://www.facebook.com/), Last accessed April 2007.

[72] *Id.*.

[73] W Roush, "Social Networking 3.0: The third generation of social-networking technology has hit the Web, and it's about content as much as contacts."
http://www.technologyreview.com/printer_friendly_article.aspx?id=15908
(accessed, 1 March, 2007). Also S Finkelstein, Blogs are no longer free from everyday commercial, Thursday 15 February 2007 pressureshttp://technology.guardian.co.uk/opinion/story/0,,2012801,00.html.

[74] *Moblogs* (http://www.moblogs.com.au/) and MMS Blogs (www.mms-blogs.com), Last accessed April 2007.

Advances in the accessibility to, and quality of, media available allow users to post their entries via various formats i.e. text, digital photography, video and/or sound files.

These sites underscore the growing acceptance by individuals that social networking sites as environments for having fun, a social ecosystem for information sharing spaces and an opportunity to make connections with the wider community.

We can draw some preliminary conclusions from this brief examination of the way individuals access new technologies 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 individuals 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. Paradoxically, the concept of privacy is being shaped by the original idea behind the web – which is to create an environment for 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, digital camera phones or wireless laptops. This is significant in the sense that data or information 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 commencing point to an answer 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 emphasise the importance of not isolating the DPD framework from the broader

relational dynamics between the individual and media. We are already witnessing some of the strategies being adopted that reflect the embryonic negotiation process being mediated by software code, contractual instrument and ideas about property. To put it another way, Article 3(2) issues are potentially being resolved through the social network spaces. For example, individuals subscribing to sites like Bebo, the host reminds its users 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.[75].

MySpace, for example has an indexing system that classifies communities through groups. For example, if an individual wanted to join a "private group" ie Article 3(2), that person would have to first become a member and login to MySpace. He would then have the option of picking a group - http://groups.myspace.com/smiles - and then apply to join the group. On moderator approval he would have access to personal information not visible to non-members.

None of the above should however detract from the transborder issues or 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:[76]

> 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

[75] *Id.*.

[76] Sylvia Mercado-Kierkegaard. *Blogs, lies and the doocing: The next hotbed of litigation? COMPUTER LAW AND SECURITY REPORT* 22(2) 127-136 [2006].

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.[77]

Bloggers, who post photos from Flickr on 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 or not they want their photographs to be accessible to the public, accessible to selected individuals or private.[78] Of particular relevance is that Yahoo may use the photograph to target advertisements based on the metadata and notes associated with the photo that is made available or the search term entered. Individuals who are in the photos may be subjected to similar advertising schemes.

Social networking spaces provide an apt illustration of how policymakers, industry and society are having 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.

A. Transborder Issues

Article 25(1) of the Directive 95/45/EC requires organisations 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 being transferred. Some blogs may have material other than texts on its site. It may contain photos, videos, pictures and audios (podcasts). Note that in some web sites which host these sites, subscribers are deemed to agree to US law rather than EU law.

From the analysis of *Lindqvist*, the ECJ holds that the uploading of webpages would not constitute the transfer of personal data as covered under Art. 25, because the provision was drafted at a time without contemplating this in mind. This does not mean that one

[77] *Id.*.

[78] *Yahoo: Flickr* (http://info.yahoo.com/privacy/us/yahoo/flickr/details.html), Last accessed April 2007.

would not be "processing" personal data as covered under the DPD, but that Art. 25 of the DPD would not, however, apply in the light of 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).[79]

B. Does the transborder transfer of personal data fall within the permitted derogations?

Two concerns can be identified. First, the principle of fairness. Second, that national governments set in place safety mechanisms for transborder transfer of personal data that are adequate. UK's approach balances the requirements of fairness and efficiency by

[79] *Lindqvist*, *Supra note*. 11, at paras. 68-71.

requiring data controllers to determine the appropriate levels of protection necessary to any particular circumstance. The conundrum here is a real one. 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. 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[80] have commented on the potential employment and intellectual property issues, defamatory and hate speech issues and privacy. 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".[81] 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.[82]

[80] This is not an exhaustive list, but see also DANIEL SOLOVE. A TALE OF TWO BLOGGERS: FREE SPEECH AND PRIVACY IN THE BLOGOSPHERE, GWU Law School Public Law Research Paper No. 207, May 7, 2006 and Ribstein, L.B. "From Bricks to Pajamas: The Law and Economics of Amateur Journalism**"** WILLIAM & MARY LAW REVIEW,(2006) *Vol. 48,* p. 185 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=700961), Last accessed April 27, 2007 and Vine, S. "Blogs, blawgs and legal issues" (2004) *EBL* 6(8) 7-9.

[81] A Hill, *This week we want to know all about... Counter-Googling*, Sunday February 11, 2007 http://technology.guardian.co.uk/print/0,,329712441-117802,00.html.

[82] Trendwatching.com. *Counter-googling* (http://www.trendwatching.com/trends/2003/09/COUNTER-GOOGLING.html), Last accessed April 27, 2007.

More importantly, can both web hosts and individuals who have blog or social networking sites be deemed to be "data controllers"? Who must be responsible for "processing"?[83] The point here is that individuals, albeit using it for personal purposes are reliant on commercial intermediaries to deal with the technical functionality. In the light of the applicable principles of fairness that provide an overarching framework, it could be argued that both sets of parties may be held accountable under the DPD.

D. Exemptions

D1 Balancing rights of expression and rights of privacy

Art. 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 (ie. that each Member State have transposed this provision differently)[84], but the ECJ was clear to emphasize that personal data does not conflict with the freedom of expression even though it may be difficult to balance the competing interests (rights of expression and rights of privacy). In a Swedish case, *Ramsbro*,[85] an individual had posted details of bank officials on the website. The purpose behind the website was to alert individuals of unscrupulous banks and unethical network-capitalists. Much of the material on the

[83] Art. 2(d) of the Data Protection Directive 95/46/EC broadly defines 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 *Lindqvist* decision as an example).

[84] See DOUWE KORFF. *STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE – COMPARATIVE SUMMARY OF NATIONAL LAWS*, (http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf) Dated May 16 2003, pp. 130-137.

[85] *Ramsbro* B-293-00, June 2001 at p. 11.

website had contained personal information which was described to be of 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 ECtHR.

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 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.[86]

The question is how do we balance the freedom of expression and the right to privacy in the blog? For example:[87]

> 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.[88]

---

[86] *Id.*.

[87] *A free man in Preston* (http://afreemaninpreston.blogspot.com/), Last accessed April 27, 2007.

[88] *Id.*.

In this example, if no one can identify who the person is, then it is not likely to fall within the scope of the Directive. However, if it can be identified who these individuals are, then this would fall within the scope of the Directive (personal data adopting a wider definition according to Art. 2(a) DPD). The question is whether this would fall outside the scope Art. 3(2) DPD? Applying a narrow interpretation, then Art. 3(2) is unlikely to apply. If steps are taken by an individual such that the webpage was not available in the public domain, there may be an arguable case that it was intended for private purposes.

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. However, as argued above, such a definition is unlikely to rest comfortably with the *Lindqvist* decision.

V. CONCLUSION

The primary argument in this paper is that 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 raise potential challenges to the existing European data protection framework and national data protection laws.[89] The *Lindqvist* decision highlights the tensions that exist with 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, there is a clear need to adopt a broader perspective of data governance and integrate

[89] By this, we are referring to EU Member States that have implemented the Data Protection Directive 95/46/EC.

businesses and consumers into the regulatory process. It is only when we recognise the paradox of new technology, its significance for the way society views privacy will we avoid the dangers identified in the Bangemann Report.[90] Art. 3(2) need to be rethought.

Europe leads the world in the protection of the fundamental rights and freedoms of the individual with regard to the processing of personal data. The application of new technologies potentially affects highly sensitive areas such as those dealing with the images of individuals, their communication, their movements and their behaviour. 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.

[90] *Europe and the Global Information Society: Bangemann report recommendations to the European Council* (http://ec.europa.eu/idabc/servlets/Doc?id=18174), Last accessed May 2, 2007.