

Data Protection confronts Freedom of Expression on the ‘New Media’ Internet: the stance of European Regulatory Authorities

David Erdos

University of Cambridge*

ABSTRACT:

European Economic Area (EEA) Data Protection Authorities (DPAs) must confront the strong tension between the EU Data Protection (DP) Directive and the public freedom of expression daily. This article is grounded on an comprehensive and original survey of EEA DPAs based on hypothetical ‘new media’ internet scenarios and demonstrates that these important regulators generally adopt an expansive interpretation of DP’s role here. Only in the case of the online media archive did a majority see the special purposes shield for journalism, literature and art (Art. 9) engaged. Default DP norms were generally held fully applicable as regards social networking sites, search engine indexers and street mapping services, whilst vis-à-vis the bloggers, social networkers and rating websites many more DPAs acknowledged that such norms required interpretation with regard for freedom of expression. There was significant diversity in response which was not directly related to divergent national transpositions of the Directive but was associated with differences in both the scope depth of the special purposes derogation in national law. This article proposes reforms aiming to ensure a more harmonized, legally certain and balanced reconciliation of rights online.

* University Lecturer in Law and the Open Society, Faculty of Law and WYNG Fellow in Law, Trinity Hall (doe20@cam.ac.uk). I am greatly appreciative to all those who aided the research presented here. In particular, I thank both Rallo Artemi Lombarte (former Director of the Spanish Data Protection Authority) and Richard Thomas (former UK Information Commissioner) for endorsing the value of the survey analysed here, the Data Protection Authorities who participated in it and both the British Academy and the Leverhulme Trust who provided much needed financial support. I also express my gratitude to Michèle Finck who gave invaluable administrative assistance on the survey, Guy Edwards who helped in the preparation of some of the statistics and Julia Powles who provided detailed comments on a previous version of this article. Any errors remain my own.

European data protection law emerged out of fears that, unless subjected to a special form of legal regulation, the rise of the computer would result in the widespread misuse of personal information to the detriment of individuals' autonomy, dignity and, especially, privacy. As a result, this law paid close attention to regulating new technological means for processing personal information, occasioning a relationship of profound tension between it and novel forms of digitally-enabled public freedom of expression, which often involved personal information processing. This 'new media' phenomena had emerged by the early 1980s in the form, in particular, of digital news archives¹ and videotex.² Nevertheless, it was the emergence of the World Wide Web on the internet from the early 1990s onwards which resulted in the explosion of ever increasingly variegated new media activity. This expansion coincided with the finalisation of a European Union (EU) Data Protection Directive 95/46, which was designed to "give substance to and amplify"³ the provisions of a 1981 Council of Europe Data Protection Convention⁴ and further the process of European harmonisation in this area. As the EU Fundamental Rights Agency has noted, since the EU "plays a pioneering role for data protection as a fundamental right and because the EU has been instrumental in driving the development of data protection systems in many Member States",⁵ the development of this body of law has broader significance for the evolution of the EU more generally, especially in the area of human rights protection.

The recent *Google Spain*⁶ judgment by the Court of Justice of the European Union (CJEU), which explored the data protection obligations of generalized search engines that index and make available information from the public domain, has dramatically highlighted the potentially severe conflicts which may arise between the pan-European data protection framework and new media internet communications. Nevertheless, the potential for such conflicts is far from limited to search engines; in fact, it arises across the entire new media internet landscape from news archiving to social networking to street mapping. As the "main actors protecting data protection rights in Europe",⁷ statutory Data Protection Authorities (DPAs) play a key role in interpreting and applying national transpositions of Directive 95/46 across this ever more complicated and important terrain. Given their central importance, this article seeks to elucidate the interpretative stance which these agencies have adopted as regards such forms of public communication. The article is based on empirical research conducted via a survey sent to European Economic Area (EEA) DPAs in 2013. In total, answers were forthcoming from 25 (over 80%) of national EEA DPAs, together with a further six operating at the sub-national level. This is the most extensive empirical survey on the subject to-date, providing an unparalleled elucidation of the current new media and data protection landscape across Europe.

The article proceeds as follows. The legal context within which the regulation of 'new media' expression under data protection must be considered is first outlined. This includes an elucidation of the general

¹ See H. Seip, "The Individual in the Age of Telematics" (1984) 7 *Transnational Data Report* 362.

² See "Preserving Data Protection in the New Media" (1983) 6 *Transnational Data Report* 416. The term 'videotex' referred to the growth of new technology providing an interactive, and at that stage largely text-based, information service via a video screen.

³ Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 1995 281/31, Recital 11.

⁴ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) (ETS 108).

⁵ European Union, Fundamental Rights Agency, *Data Protection in the European Union: the role of National Data Protection Authorities* (2010), p. 50, http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf [accessed May 16, 2015].

⁶ *Google Spain, Google v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez* (C-131-12), EU:C:2014:317.

⁷ European Union, Agency for Fundamental Rights, *Access to Data Protection Remedies in EU Member States* (2013), p. 49, http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf [accessed May 16, 2015].

scope and substance of data protection, together with an analysis of legal debate concerning its interaction with freedom of expression at the time when Directive 95/46 was finalized and also during and subsequent to the seminal CJEU *Lindqvist*⁸ judgment. Details are then provided of the survey sent to EEA DPAs together with its rationale. The specific hypothetical ‘new media’ scenarios included in the survey, which concerned a traditional media story, media archive, amateur blogger, social networker, social networking site, rating website, search engine and street mapping service, are discussed. In addition, the particular legal questions put before DPAs are explicated. Following on from this, the article elucidates, both in general and as regards each particular scenario, the responses received from the DPAs. An analysis of these results is then provided, including a probing of whether the variation of DPA approaches may be related to divergences in national legal transposition of the Directive 95/46, whether these stances are compatible with binding CJEU jurisprudence, and how in the context of the proposed new Data Protection Regulation⁹ the understanding of DPAs in this area might be subject to change in order to better account for freedom of expression in the evolving digital environment. The article closes with some brief conclusions.

The Legal Context

The Data Protection Framework

As Lord Leveson stated in the UK inquiry in to the culture, practices and ethics of the press, data protection is often “viewed as marginal” by legal practitioners including the higher courts.¹⁰ In reality, however, the EU Data Protection Directive 95/46 which was finalized in 1995 has a breath-taking material, purposive and substantive reach. Article 3.1 sets out its default material scope as encompassing the “processing of personal data wholly or partly by automatic means” as well as in certain structured, manual filing systems. All of these key terms are defined expansively. Thus, “processing ... by automatic means” includes “any operation” performed digitally including collection, retrieval, consultation, dissemination and erasure.¹¹ “Personal data” refers to “any information relating to an identified or identifiable natural person (‘data subject’),”¹² a terminology capacious enough to even encompass innocuous public domain material, perhaps even as anodyne as the name of an author coupled with a book title.¹³ Meanwhile, Article 1 states that the purpose of the law is to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”, at the same time prohibiting the restriction of the free flow of such information within the European Economic Area (EEA) for reasons connected with such protection.¹⁴ As a result of these broad purposes, data “controllers” – that is anyone “who alone or jointly with others determines

⁸ *Criminal proceedings against Bodil Lindqvist* (C-101/01) EU:C:2003:596.

⁹ European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* (COM (2012) 11 final)).

¹⁰ B. Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (London: The Stationary Office) (2012), p. 999.

¹¹ Directive 95/46, art. 2 (d).

¹² *Ibid.*, art. 2 (a).

¹³ “Amendments Likely on Data Protection”, *Bookseller*, 5 July 1991, p. 8.

¹⁴ Although the wording on the face of Directive 95/46 only refers to the European Union, the Agreement on the European Economic Area (OJ 1994 L 1/7) extends the Directive to three associated states (Iceland, Liechtenstein and Norway) which, together with the EU, make up the European Economic Area (EEA).

the purposes and means of the processing of personal data”¹⁵ – are bound to set of stringent default substantive provisions. These provide that, absent a special derogation or exemption, data processing must comply as necessary with:

- *data quality principles* such as fairness, non-excessiveness and accuracy,¹⁶
- *transparency rules* setting out detailed proactive and retrospective requirements for ensuring the openness of processing vis-à-vis the data subject,¹⁷
- *sensitive data rules* which generally ban the processing of criminal, health, political opinion, ethnic and certain other broad categories of information within the private sector unless this prohibition has been waived by the subject, either through express consent or through them “manifestly” making the data public,¹⁸ and
- *control conditions* which impose additional restrictions, such as regards data export and data security, with a view to ensuring that the other elements of the scheme are not undermined.¹⁹

Turning to the supervisory system, Member States must, in addition to providing a direct judicial remedy,²⁰ establish one or more independent Data Protection Authorities (DPAs) and endow the same with wide-ranging powers and duties to monitor application of the law and hear claims lodged by data subjects.²¹ Following the adoption of Directive 95/46, in 2000 the EU also adopted Directive 2000/31 which set out a generally overarching framework for “information society services”.²² This e-Commerce Directive *inter alia* shielded, albeit only in qualified terms, certain so-called “intermediary service providers” from legal liability; such providers were defined as those which were mere conduits or which were only engaged in the caching or hosting of material.²³ Importantly, however, as a result of Art. 1.5(b), data protection responsibilities were excluded from the ambit of Directive 2000/31. In the same year, the EU also drafted a Charter of Fundamental Rights including within it a right to the protection of personal data.²⁴ The Treaty of Lisbon, which entered into force in December 2009, provided that a slightly revised version of this Charter,²⁵ still including a right to data protection, had the same legal status as the EU Treaties.²⁶ It also separately provided that “[e]veryone has the right to the protection of personal data concerning them”.²⁷ At the least, the presence of these fundamental rights guarantees impacts on context within which the more detailed provisions found in Directive 95/46 must be interpreted.²⁸

¹⁵ Directive 95/46, art. 2 (d).

¹⁶ Ibid, art. 6.

¹⁷ Ibid, arts. 10 - 12.

¹⁸ Ibid, art. 8.

¹⁹ Ibid, art. 7, art. 17, art. 18 – 21 and arts. 25 – 26.

²⁰ Directive 95/46, art. 22.

²¹ Ibid, art. 28. The latter are also empowered with a range of specific remedial rights which, in general, can lead also lead to action either in court or before the DPA.

²² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (‘Directive on electronic commerce’), OJ 2000 L 178/1.

²³ Ibid, art. 12-15.

²⁴ P. Craig and G. De Burca, *EU Law: Text, Cases and Materials*, 4th edn. (Oxford: OUP, 2011), p. 394.

²⁵ OJ 2010 C 83/389.

²⁶ TEU, Art. 6.1.

²⁷ TFEU, Art. 16.

²⁸ It should, however, be noted that these new provisions do not formally bind the three EU-associated states of Iceland, Liechtenstein and Norway.

The Original Debate on Public Freedom of Expression under Directive 95/46

The structure of European data protection places it in clear tension with public freedom of expression, which may be conceptualized as encompassing the freedom to disclose to an indefinite number of people “information and ideas without interference by public authority and regardless of frontiers” coupled with the right of these people to receive the same material.²⁹ This tension was recognised during the drafting and transposition of Directive 95/46 but only as regards a specially defined area of expression. In the European Commission’s original proposal, this area was delimited institutionally so as to shield processing “in respect of the press and the audiovisual media”.³⁰ During the subsequent negotiations, however, the phrasing was expanded to encompass all “processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression”.³¹ Within this special purposes area, EEA Member States were obliged to provide derogations but “only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression”³² or, in different phraseology, only as “necessary for the purpose of balance between fundamental rights”.³³ Although other parts of the Directive did enable Member States to adopt more limited derogations where “necessary ... to safeguard ... the rights and freedoms of others”,³⁴ public freedom of expression was rarely discussed in this context. Moreover, notwithstanding its clear potential applicability in this area, Member States have generally³⁵ not utilized such provisions in order to adopt protections for public freedom of expression which go beyond the special purposes as they have delimited them. (As will be seen below, this delimitation nevertheless differs substantially between the EEA jurisdictions at national level).

Debate on Public Freedom of Expression in Lindqvist and beyond

Notwithstanding the essentially dichotomous original conceptualisation of the relationship between data protection and public freedom of expression instantiated in Article 9 of Directive 95/46, the *Lindqvist* case vividly illustrated early on in the Directive’s history that understandings of how to best to reconcile these two legal values was in fact much more variegated and diverse. This case concerned the relationship between data protection and Mrs Lindqvist’s publication on her personal internet site of “personal data on a number of people

²⁹ European Convention on Human Rights 1950 art. 10; Charter of Fundamental Rights of the European Union (O. J. 2010 C 83 p. 389), art. 11. Freedom of expression includes within itself a distinct informational sub-right which comes into particular conflict with data protection. This sub-right is explicitly recognised in art. 11 of the EU Charter through its heading “[f]reedom of expression and information”.

³⁰ ‘Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data’ COM (90) 314 final OJ 1990 C 277/3, art. 19.

³¹ Directive 95/46, art. 9.

³² Ibid, art. 9.

³³ Ibid, Recital 37.

³⁴ See, in particular, Directive 95/46, art. 13 (g). Whilst this provision does not provide for any derogation from the sensitive data rules, articles 8.4 and 8.5 do allow Member States to derogate from these restrictions for reasons of “substantial public interest” and subject to the provision of “suitable safeguards” or, in the case of restrictions applicable to data relating to offences, criminal convictions or security measures, subject to “suitable specific safeguards”.

³⁵ The only important exception to this is a 2007 amendment adopted in Sweden which excluded from all the substantive provisions of its Personal Data Act processing which “is not intended to be included in a collection of personal data which has been structured in order to evidently facilitate search for or compilation of personal data” and does not violate the privacy of the data subject (Sweden, *Personal Data Act* 1998, s. 5 (a)).

working with her on a voluntary basis in a parish of the Swedish Protestant Church”.³⁶ Mrs Lindqvist herself argued that given that her processing was “free of charge and unconnected with any economic activity”,³⁷ she could rely on Article 3.2 of Directive which completely exempts both processing “in the course of an activity which falls outside the scope of Community law” and processing “by a natural person in the course of a purely personal or household activity”. The European Commission rejected these claims but argued that, “given the purpose of the internet page at issue”, it constituted “an artistic and literary creation [sic] within the meaning of Article 9 of that Directive”.³⁸ Whilst not endorsing this proposition, the Netherlands Government argued that, given that freedom of expression was clearly engaged, “the national court must endeavour to balance the various fundamental rights at issue by taking account of the circumstances of the individual case”.³⁹ Finally, the United Kingdom Government implied that the general provisions of European data protection could legitimately apply in full.⁴⁰

The CJEU judgment clearly rejected the notion that Lindqvist was exempted from the Directive under Article 3.2. The Court claimed that the first indent of this provision was limited to “activities of the State or of State authorities”⁴¹, and that the second indent must be confined “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”.⁴² The Court also declined to agree with the Commission that Article 9 was engaged. Nevertheless, in the process of rejecting Mrs Lindqvist’s contention that Directive 95/46 directly violated freedom of expression and other related rights,⁴³ it did acknowledge that “Mrs Lindqvist’s freedom of expression and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of individuals about whom Mrs Lindqvist has placed data on her internet site”.⁴⁴ As a result, the Court argued that “it is for the authorities and courts of the Member States ... to make sure they do not rely on an interpretation of [the Directive] which would be in conflict with the fundamental protected by the Community legal order or with the other general principles of Community law, such as *inter alia* the principle of proportionality”.⁴⁵

Notwithstanding the apparent clarity of aspects of the *Lindqvist* judgment, the various issues raised in the case remain unresolved in practice. Some key actors continue to argue that, as a result of Article 3.2, certain new media activities are entirely exempted from data protection, irrespective of the fact that they necessarily disseminate personal information to an indefinite number of persons. For example, the UK DPA states that it “will not consider complaints made against individuals who have posted personal data whilst acting in a personal capacity, no matter how unfair, derogatory or distressing the posts may be. This is because where an individual is posting for the purposes of their personal, family[, household or recreational purposes the ...

³⁶ *Lindqvist* (C-101/01) EU:C:2003:596 at [2].

³⁷ Opinion in *Criminal proceedings against Bodil Lindqvist* (C-101-01), EU:C:2002:513 at [29].

³⁸ *Lindqvist* (C-101/01) EU:C:2003:596 at [33].

³⁹ *Ibid* at [76].

⁴⁰ *Ibid* at [55].

⁴¹ *Ibid* at [43].

⁴² *Ibid* at [47].

⁴³ *Lindqvist* (C-101/01) EU:C:2003:596 at [73]-[74].

⁴⁴ *Ibid* at [86].

⁴⁵ *Ibid* at [87].

exemption will apply”.⁴⁶ The types of new media activity which can benefit from the special purposes shield also remains disputed. In *Satamedia* the CJEU stated that “[i]n order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary ... to interpret notions relating to that freedom, such as journalism, broadly”⁴⁷ and, in particular, held “activities involving the processing of personal data” must be considered as carried out “solely for journalistic purposes” if “the sole object of those activities is the disclosure to the public of information, opinions or ideas”.⁴⁸ A number of commentators interpreted this latter definition very expansively, with Lynskey even holding that it encompassed “any form of expression involving personal data processing”.⁴⁹ Nevertheless, in *Google Spain*, the CJEU was clear that it did not extend to either the supply by, or receipt from, a general search engine of public domain information.⁵⁰ Finally, the circumstances in which it is appropriate to have explicit regard for freedom of expression when applying general data protection law also remains controversial. Thus, Rallo and Martinez (2014) argue that, as regards indeterminate publication by an individual on a social networking site, “the conflict between the right to data protection and the freedom of expression or right to information must be resolved by the competent authority or national judge”.⁵¹ In contrast, Van Alsenoy et. al. (2009) detail the extensive legal liabilities faced by such social network users under general data protection provisions, without any acknowledgment that there may be requirement to ‘read-down’ these provisions in order to have regard for freedom of expression here.⁵²

The EEA Data Protection Authority Survey

As has been widely noted in the literature, in practice, it is the statutory Data Protection Authorities (DPAs) which play the leading role in the realisation of Directive 95/46. Indeed, Blume and Svanberg (2013) even state that “[t]he credo is that without the agency, there is no data protection”.⁵³ The centrality of the DPAs is also reflected in the fact that one of the few elements of the data protection regime which is specifically entrenched in the *EU Charter* is that “[c]ompliance ... shall be subject to control by an independent authority”.⁵⁴ In recognition of their key role, the study aimed to explore the legal understandings of these agencies as regards ‘new media’ internet expression. This task was approached through the development of a survey sent to both

⁴⁶ UK, Information Commissioner’s Office, *Social Networking and Online Forums – When Does the DPA Apply?* (n. d.), <https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf> [last accessed May 16, 5 November 2014]. This position has been maintained despite the CJEU clearly restating this aspect of the *Lindqvist* case in the later case of *Satamedia*. See *Tietosuoja- ja valtuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* (C-73/07) EU:C:2008:727 at [44].

⁴⁷ *Lindqvist* (C-101/01) EU:C:2003:596 at [56].

⁴⁸ *Satamedia* (C-73/07) EU:C:2008:727 at [61]. The definition provided by the Court here was, in theory, limited to processing “relating to documents which are in the public domain under national legislation” [Ibid].

⁴⁹ O. Lynskey, “From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection’s Identity Crisis” in S. Gutwirth, R. Leenes, P. de Hert and Y. Pouillet (eds), *European Data Protection: Coming of Age* (Dordrecht; New York: Springer, 2013), p. 71.

⁵⁰ *Google Spain* (C-131/12) EU:C:2014:317 at [85].

⁵¹ A. Rallo and R. Martinez, “Protecting personal data and media networks” (2011) 14 *Quaderns Del Cac* 37.

⁵² B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, “Social Networking and Web 2.0: Are Users also Bound by Data Protection Regulations?” (2009) 2 *Identity in the Information Society* 65.

⁵³ P. Blume and C. Svanberg, ‘The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Divide and the Bureaucratic Apparatus’ (2013) 15 *CYELS* 40.

⁵⁴ EU Charter, art. 8.3.

national and sub-national EEA DPAs,⁵⁵ initially in March 2013, with replies being received until the end of July 2013.

Turning to the construction of the survey itself, the term ‘media’ expression was conceptualized as referring to mass communication or, in others words, forms of disseminating information to a potentially large and generally indefinite number of people.⁵⁶ Meanwhile the focus on the ‘new’ as opposed to the ‘traditional’ media was designed to focus on “those methods and social practices of communication ... that have developed using the digital, multimedia, networked computer and ways in which this machine is held have transformed work in other media.”⁵⁷ In light of the fact that this “apparently unifying term ... actually refers to a wide range of changes in media, production, distribute and use”,⁵⁸ it was realised that it was necessary to present DPAs with a broad range of ‘new media’ scenarios. In addition, a scenario limited to the ‘traditional’ media was crafted to act as a control. In sum, the various hypothetical scenarios which were put before DPAs were as follows:

0. **Traditional media (Control):** “[A] media entity produc[es] a story concerning a living individual[.]”
1. **Newspaper archive:** “A searchable online newspaper archive publishes a newspaper story originally published a decade ago concerning a living individual.”
2. **Individual blogger:** “In his spare time, an individual publishes a blog that discusses and disseminates gossip about various celebrities. It is freely available on the Internet and visited by several hundred people a week.”
3. **Rating website** - “A company establishes a website freely available on the Internet allowing individuals to ‘rate’ and add comments about their teachers.”
4. **Social networker:** “A member of a Social Networking Site (SNS), the membership of which is generally open to individuals worldwide, ‘tags’ a photo of an identified individual and makes an informed decision to make this freely available to all members of the site.”
5. **Social networking site (SNS):** “The Social Networking Site (SNS) is contacted directly by the same identified individual as above [i.e. the data subject mentioned in scenario 4 above] who claims that the Site itself is a Data Controller in relation to this processing.”
6. **Search engine** - “A company provides a service allowing people to search the information sources of the public Internet (including on identified individuals) through a web-based search engine.”
7. **Street mapping service** - “A street mapping service produces maps with street-level photographic images including pictures of individuals, motor vehicles and homes.”

As regards each of these scenarios, the DPAs were asked to indicate which one of the following alternative legal statements was considered to be correct:

- a. Data protection does not apply.

⁵⁵ Sub-national DPAs have been established in Spain and Germany as well as in Gibraltar, a British Overseas Territory within the EEA with a data protection regime which is separate from that of the mainland UK. For the status of Gibraltar within the EEA see TFEU, art. 553 (3).

⁵⁶ It is in this sense that the Oxford English Dictionary defines the media as “[t]he main means of mass communication, *esp.* newspapers, radio, and television, regarded collectively”.

⁵⁷ M. Lister, J. Dovey, S. Giddings, I. Grant and K. Kelly, *New Media: A Critical Introduction* (London: Routledge, 2003), p. 2.

⁵⁸ *Ibid.*, p. 13.

- b. Data protection applies, but the activity in question must benefit from all the special purposes derogations and exemptions for journalism, art and literature envisaged in Article 9 of Directive 95/46/EC.
- c. The general provisions of data protection apply, but must be interpreted with regard for other fundamental rights including freedom of expression.
- d. The general provisions of data protection law apply in full.⁵⁹

In place of such a standard categorical response, DPAs were able to state that the activity “has a different relationship with data protection” and provide a free-text specification of this.⁶⁰ Some DPAs also provided specific additional text specification alongside a categorical response. Both the categorical responses and the qualitative answers will be explored below.

The seven ‘new media’ scenarios were primarily formulated so as to cover a cross-section of those types of new media activity which have become well-established and ubiquitous. At the same, they were also constructed to probe the DPA’s understanding of the relevance or otherwise of particular types of divergence from ‘traditional’ media practice. The following dimensions of divergence have assumed particular prominence within the ‘new media’ space:

- Changes in the type of *information actor*. This has variously involved the presence of a new individual actor engaged in mass communication (as in scenarios 2 and 4) or a new corporate actor with the potential to structure the general nature of such activity (as in scenarios 3, 5, 6 and 7).
- Changes in *information context*. In particular, there has been a shift from information dissemination being temporally and semantically situated in discrete articles, programmes and other works to being increasingly integrated into electronic data banks, capable of permanently and seamlessly serving up large amounts of information on individuals on a granular basis. Whilst such a transformation is not so evident in scenarios 2 and 7,⁶¹ it is particularly stressed in the other cases.
- Changes in *information focus*. Whilst the traditional media published material based on its allegedly legitimate interest for the collective public, many ‘new media’ activities are justified largely on the basis that they are linked to individual self-expression⁶² or that they provide what is

⁵⁹ The question put to DPAs as regards the traditional media control scenario (example (0)) was deliberately placed elsewhere in the survey and also phrased slightly differently. This question asked: “Do the activities of a media entity producing a story concerning a living individual fall within the scope of Data Protection law? Please tick one answer”. Four options were set out: “Yes” (a cognate to ‘new media’ statement (d)), “Yes, however, Data Protection must be interpreted with regard for potentially conflicting rights to freedom of expression” (a cognate to ‘new media’ statement (c)), “Yes, but the media entity must benefit from all the special derogations and exemptions for journalism, art and literature envisaged in Article 9 of Directive 95/46/EC” (a cognate to ‘new media’ statement b) and “No” (a cognate to ‘new media’ statement (a)).

⁶⁰ In relation to the control scenario (example (0)) DPAs were not formally invited to provide such a non-standard answer. Despite this, a number nevertheless elected to do so.

⁶¹ The production of a blog (scenario 2) does not necessarily indicate that the publisher is taking any steps to ensure the indexing of personal information. Even more clearly, whilst a street mapping service (scenario 7) does capture personal images, its photographs are only designed to be searchable as regards information which is not necessarily personal (e.g. a particular address or landmark).

⁶² For example, Lord Allen, Facebook’s Director of Policy in Europe, has equated expression on the platform with “people speaking in a pub, a bar, a marketplace or a football match. They are speaking in a quite different tone and context from anything that we have ever had before. To treat that kind of speech identically to that made in the *Times* or on the BBC misjudges what is taking place” (United Kingdom, Parliament, House of Lords, *Debates*, 19 December 2012, col. GC573

essentially a privatised service (in other words, a facility which is primarily designed to further a private interest of the corporate or individual end-user).⁶³

Table 1 below provides a graphical representation of those aspects of the divide between the ‘new’ as opposed to the ‘traditional’ media which these scenarios particularly explored. Whilst a tick (✓) indicates an aspect clearly present in the example and a cross (✗) an aspect definitely not present, a hyphen (-) signifies uncertainty. The shaded area represents a shift from the traditional media context.

Table 1: Mapping the contours of the ‘new media’ scenarios

Dimension →	Information Context		Information Actor			Information Focus		
	Situated	Integrated	Corporate ‘Old Media’	Individual ‘New Media’	Corporate ‘New Media’	Collective Public Interest	Individual self-expression	Private service
Scenario ↓								
(1) Media archive	✗	✓	✓	✗	✗	✓	-	-
(2) Amateur Blogger	-	-	✗	✓	✗	✓	✓	✗
(3) Rating Website	✗	✓	✗	✗	✓	✗	✓	✓
(4) Social Networker	✗	✓	✗	✓	✗	✗	✓	✗
(5) SNS	✗	✓	✗	✗	✓	✗	✓	-
(6) Search Engine	✗	✓	✗	✗	✓	✓	✓	✓
(7) Street Mapping	-	-	✗	✗	✓	✗	✗	✓

Turning to the crafting of the alternative categorical legal statements which DPAs were asked to assent to, these were essentially designed to crystallize the four broad approaches to the interface between media activity and data protection which were put before the CJEU in the *Lindqvist* case. In essence, these options represent ordered categories ranging from no application (option (a)) through to full application (option (d)) of the default European data protection framework. Given this, it is possible to translate the responses on to quantitative scale ranging from 0 (no application) to 1 (full application) of data protection, where (a) is equal to 0, (b) to 0.33, (c) to 0.67 and (d) to 1. This translation has particular value since, as will be elucidated in the analysis part of this article below, it enables certain statistical calculations to be performed.

The EEA Data Protection Authority Survey Results

General Overview and Elucidation of Responses

Replies to the survey were received from 25 (over 80%) of national DPAs together with a further six authorities operating at the sub-national level. Table 2 below sets out all of the basic information on these

(Lord Allen of Hallam)). This sentiment chimes with Facebook’s mantra of “[m]aking the Web more social” (J. Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford: OUP, 2013), p. 11).

⁶³ For example, Google Alerts, a system which allows customers to receive weekly, daily or even “as it happens” reports from Google from its search engines, has been specifically advertised for *inter alia* “keeping current on a competitor” (Google, ‘Google Alerts – Monitor the Web for Interesting New Content’ (2014), <https://web.archive.org/web/20140527082344/http://www.google.co.uk/alerts> [accessed May 16, 2015]).

responses. In relation to each scenario, the first column sets out the total number of responses received, the number of categorical responses (including where specific additional text was also provided) and the number of qualitative free-text answers. As can be seen, in each case, between 86% and 100% of the responses were in the form of the pre-formulated standard, and therefore quantifiable, categories. Turning to these responses only, the next four columns detail both the percentage and total number falling within each of the four standard categories. (These results are also specified at individual DPA level in the appendix to this article). The last column then provides an overall score for each scenario, computed from an averaging of all the categorical responses as translated into the 0, 1 scale detailed above. In effect, this score measures the extent to which DPAs as a whole understood that the norms of data protection were engaged in the scenario in question. In principle, and similarly to the categories themselves, this score could range from a total absence of acknowledged engagement (0) through to an understanding that the data protection norms were fully engaged (1). In fact, since replies to all the scenarios featured responses in more than one of the standard categories, this score was not only never at these extremes but also was never precisely the quantitative cognate of any of the four categories themselves. Despite this, these values usefully can be rounded to the most applicable category. In this way, a value of 0 – 0.17 rounds to category a/0 (representing ‘negatory’ engagement of DP norms), a value of > 0.17 – 0.5 to category b/0.33 (representing a ‘limited’ engagement), > 0.5 – 0.84 to category c/0.67 (representing an ‘extensive’ engagement) and > 0.84 – 1 to category d/1 (representing a ‘comprehensive’ engagement). The outcome of such a rounding is also specified in the last column. (Given that this rounding of the average of mean values often differed from the modal categorical average - in other words, the category in which the DPA at the mid-point of the responses was located - this is separately highlighted through a bolding of the relevant value.) The last column also sets the standard deviation of the quantified categorical responses as regards each scenario. This figure provides an important measure of the extent to which DPAs either tended to agree on a common approach, which is signified by a smaller standard deviation score, or by contrast indicated disparate responses, which produces a much higher score. Finally, the last row of the table sets out combined information on responses to all the ‘new media’ scenarios (examples (1) – (7)) including an average of the number of different types of responses received, average standard responses in each category, the average data protection engagement score and the average standard deviation. In addition, the average data protection engagement score (0.75) is rounded to the nearest whole category (category c/0.67) and the modal categorical value for all the scenarios combined (category d/1) separately highlighted in bold.

Table 2: Summary of Total Responses to EEA DPA Survey

New Media Example	Responses: Total; Categorical (with text); Free-text	Exempt/ Nugatory Engagement Category (a/0)	Special Derogation/ Limited Engagement Category (b/0.33)	Regard for Expression/ Extensive Engagement Category (c/0.67)	Full Application/ Comprehensive Engagement Category (d/1)	Data Protection Engagement Score (Nearest category) (Standard Deviation)
(0) Media Story	30; 27 (3); 3	4% (1)	67% (18)	26% (7)	4% (1)	0.43 (b) (0.20)
(1) Media Archive	29; 25 (0); 4	12% (3)	48% (12)	32% (8)	8% (2)	0.45 (b) (0.26)
(2) Amateur Blogger	29; 25 (2); 4	12% (3)	24% (6)	60% (15)	4% (1)	0.52 (c) (0.25)
(3) Rating Website	30; 30 (2); 0	3% (1)	0% (0)	50% (15)	47% (14)	0.80 (c) (0.22)
(4) Social Networker	29; 25 (2); 4	16% (4)	4% (1)	32% (8)	48% (12)	0.71 (c) (0.36)
(5) SNS	29; 26 (4); 3	0% (0)	4% (1)	23% (6)	73% (19)	0.90 (d) (0.18)
(6) Search Engine	29; 26 (0); 3	8% (2)	0% (0)	12% (3)	81% (21)	0.89 (d) (0.28)
(7) Street Mapping	30; 29 (0); 1	0% (0)	0% (0)	7% (2)	93% (27)	0.98(d) (0.08)
(1)-(7) Average	29; 27 (2); 3	<u>7%</u>	<u>11%</u>	<u>31%</u>	<u>51%</u>	<u>0.75 (c) (0.23)</u>

Elucidation of Responses to each New Media Scenario

It is clear from the last column of Table 2 that there was no situation where a rounding of the data protection (DP) engagement score indicated that DPAs generally considered data protection law to be in principle inapplicable (category a/0). Instead, if this score is prioritized, the scenarios divide broadly into three groupings, comprising examples zero and one (which round to category b/0.33), two to four (which round to category c/0.67), and five to seven (which round to category d/1) respectively.

Turning to the first grouping, in the case of both the media story control scenario (example (0)) and the media archive scenario (example (1)), DPAs tended to accept that, whilst data protection law was in principle applicable, the special purposes derogation (b/0.33) was also engaged. As regards the media story, unsurprisingly given the clarity of Directive 95/46 on this point, the clear majority (67%) of standard responses selected this category. Nevertheless, as detailed in Chart 0 below, at least one DPA also selected each of the other categories. This resulted in an overall DP engagement score of 0.43. In addition, despite indicating that the special purposes provision was engaged, the Hungarian DPA added additional text which somewhat limited its scope.⁶⁴ In sum, it stated:

⁶⁴ On the other hand, the Cypriot DPA which stated that data protection was fully applicable (1/d) included further text indicating that a public interest balancing was nevertheless acceptable. In sum, it stated “[i]n every case, data published for journalistic purposes should obey the principle of proportionality. To strike the right balance between the public’s right to information and the data subject’s right to privacy, the following criteria should be taken into account to determine what is proportional to publish: (i) the public’s particular interest for a specific story, at the time of publication (ii) if the story involves a public figure or an average person and (iii) if the nature of the story justifies the public’s overriding right to be informed of the persons’ names involved in the story. For example, a newspaper publishes today an article on a well known doctor, who is named, accused for tax evasion. While the current economic situation in Cyprus and the public’s sensitivity on this type of stories today seem to justify the publication, few years ago, naming the doctor would have been in breach of the proportionality principle”. Finally, the Polish DPA (b/0.33) simply provided a translation of the special purposes provision set out in Polish data protection law.

[I]t is not the general Privacy Act (Act CXII of 2011) but the Act CIV of 2010 on Freedom of the Press and on the Basic Rules Relating to Media Content which provide a special legal protection for journalists and the sources they use in their investigation activities. Therefore the Act on the Freedom of the Press shall be applied as *lex specialis* compared with the Privacy [Data Protection] Act. ... On the other side it has to be underlined that the special legal protection of the journalists is only in relation with ‘public data of public interest’, which also covers personal data that are made public by virtue of a public interest (e.g. relevant personal information of a politician or other public figure). If the data controlled by the journalists does not qualify as data of public interest in relation with freedom of information general data protection regulation applies.

This spread of responses was not subject to significant modification as a result of the three free text answers which were also received.⁶⁵ Turning to the media archive scenario (example 1 – Chart 1 below), the small difference in the overall DP engagement score between this and the media control scenario (0.45 as opposed to 0.43) indicates that, notwithstanding the significant change in information context brought about by this new media activity (see Table 1), DPAs generally saw the two cases as being legally comparable. Nevertheless, the fact that only a plurality as opposed to significant majority of responses directly selected the special purposes category is indicative of a considerably greater diversity of interpretation here. This is also reflected in a substantial increase in the standard deviation (0.26 compared to 0.20). Albeit with certain caveats, the free-text responses also tended to link this activity back to the traditional journalistic context. The Slovenian DPA response was essentially the same as that provided for the control scenario.⁶⁶ Similarly, the German Länder of Rhineland-Palatinate DPA stated that “journalistic activities are without the control of the data protection authority; the data protection law is not applicable. But the journalist has to comply with the fundamental rights of personality, the right to determine about one[']s own pictures and the civil law concerning damages (§§ 823, 826 German Civil Law)”. The Austrian DPA simply provided an English translation of the section of its national data protection act headed “[j]ournalistic purposes”, noting that the relationship between data protection and the media was regulated by this. Finally, and rather more ambiguously, the Portuguese DPA provided a lengthy response which *inter alia* stated that:

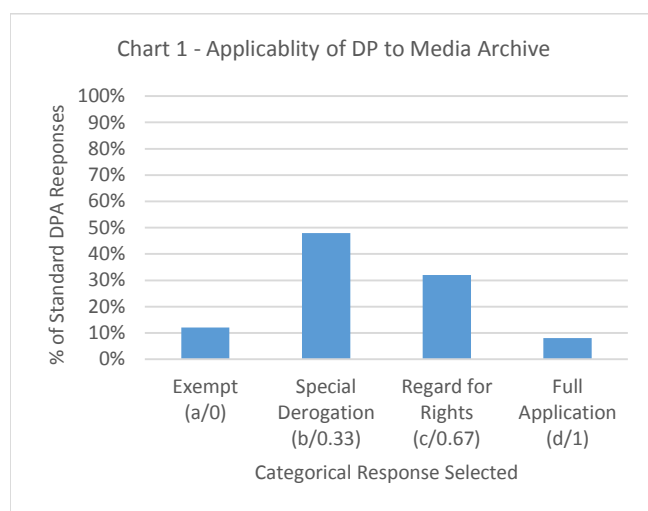
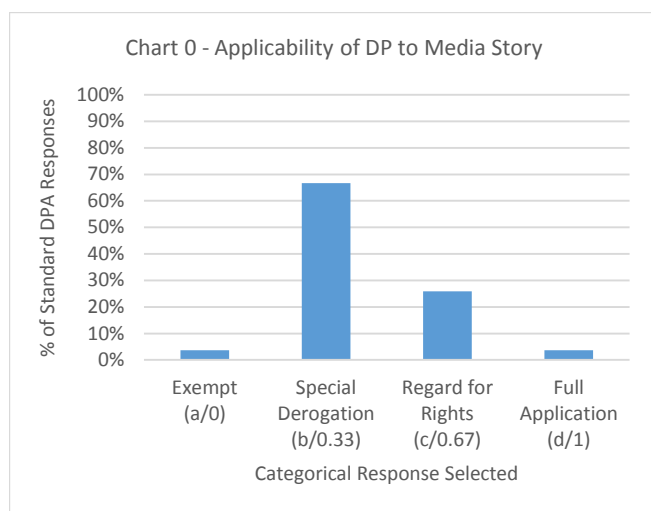
Newspaper archives could always be searched before the Internet. The availability of online archives is a way of facilitating the public access to information. They simply reflect what was published in paper, properly dated, and the due accuracy of the moment ... Nevertheless, considering the lack of update and the lack of consent from the data subject, and having [taken] into consideration the huge negative impact that some news may have to an individual (for instance, in case of a person that was

⁶⁵ The German Länder of Rhineland-Palatinate DPA indicated that data protection applied “but there are also media-specific laws” (see also the later response to media archive scenario which indicated that data protection was applicable only in areas such as administration and not as regards journalistic activities per se). The Slovenian DPA adopted a highly idiosyncratic approach stating that data protection would apply in full “if the published data is such that would be protected under data protection law, e.g. if it has been acquired from a data controller and published without legal grounds. In other cases the general law on defamation and breach of privacy applies. Our law does not include the exemption for journalism, art and literature.” Finally, the thrust of the UK DPA’s response appeared to accept the applicability of the special purposes derogation stating that “such activities would almost certainly involve the processing of personal data for the purposes of the Data Protection Act 1998. However, the so-called special purposes exemption in section 32 of the Act is likely to be engaged and will have some impact on how the provisions of the DPA [Data Protection Act] apply to the specific circumstances.”

⁶⁶ In sum, it stated that data protection would apply in full if “the published data is such that would be protected under data protection law, e.g. if it has been acquired from a data controller and published without legal grounds. In other cases, where the data does not originate from a certain data controller, the general law on defamation and breach of privacy applies.”

prosecuted and then acquitted), it is our understanding that the newspapers['] online archives should not be indexed to the search engines, as this would be potentially damaging to a person's reputation and dignity in a larger scale.

Overall, the narrow nature of this first grouping suggests that DPAs tend to interpret the special purposes category so that it is confined primarily to traditional journalistic entities in the press and broadcasting sector.



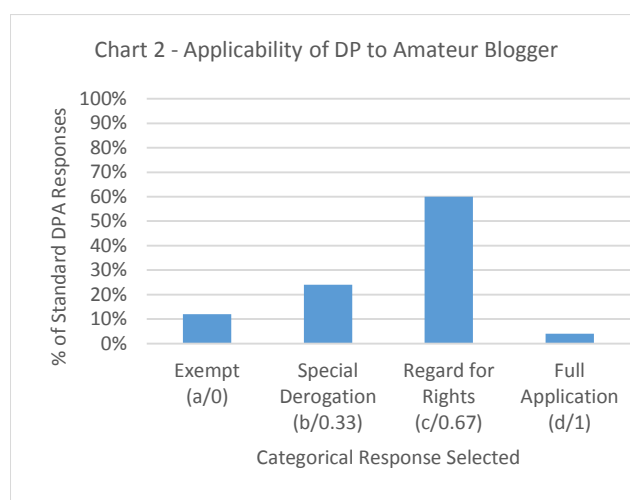
Secondly, there is a group of three scenarios (which relate to an amateur blogger, social networker and rating website) (examples two to four) where a rounding of the DP engagement score suggests that the general data protection provisions should apply but that these must be interpreted with regard for freedom of expression and related rights (category c/0.67). Despite these commonalities, however, there are also significant divergences here, both as regards the cases themselves and as regards the nature of responses received. The amateur blogger scenario (example 2; Chart 2) was the only one where a significant minority of DPAs (24% of standard responses) still considered the special purposes derogation (b/0.33) applicable. This may be related to the fact that, uniquely amongst this group, the blog's information focus ('celebrity gossip') is one which the traditional media has sought to justify as being in the collective public interest. The case also does not highlight a shift in informational context.⁶⁷ Despite this, a majority of standard responses (60%) held that the general data protection provisions still applied and only needed to be interpreted with regard for freedom of expression (c/0.67). A few DPAs also selected the other categories, resulting in a DP engagement score of 0.52 and a standard deviation of 0.25. With the exception of the Slovenian DPA response,⁶⁸ the qualitative information provided by DPAs also displayed some uncertainty as to how amateur blogging should be regulated. Whilst the Cypriot DPA argued that data protection was fully applicable (d/1), it included two texts which appeared to qualify this considerably:

⁶⁷ See Table 1 and footnote 61.

⁶⁸ The Slovenian response was largely identical to that in examples 0 and 1 above. In sum, it stated that data protection law would apply in full "if the published data is such that would be protected under data protection law, e.g. if it has been acquired from a data controller and published without legal grounds. If it is merely gossips, not originating from a certain data controller, the general law on defamation and breach of privacy applies".

As a rule, the exemption of journalistic purposes (freedom of expression) should also be applied to persons who are not journalists by profession but publish data in relation to cases for which there is an increased journalistic public interest at the time of publication Discussing gossips does not necessarily imply the processing of personal data. Re-publishing personal data made publicly available by other media would not be in breach of the Law unless the Commissioner ascertains a contravention of the Law in line with section 4(2) of the DP [Data Protection] Law.

The Estonian DPA stated that the special purposes derogation was applicable (b/0.33), but in free-text also indicated that “the practice” of the authority additionally took into account the criteria of interpreting general data protection with regard for freedom of expression (c/0.67). The Austrian DPA stated both that data protection was fully applicable (d/1) and that the activity had a different relationship with the law from the standard categories, adding text which indicated that whilst a special section of the national law regulated the relationship between data protection and the media “[t]he regular Data Protection Act may apply to blogs and similar less regulated ‘media’”. Somewhat similarly, whilst indicating the special purposes derogation was applicable (b/0.33), the German Länder of Rhineland-Palatinate DPA stated that if the blog could be classified as journalistic activity it only had the capacity to control the blogger “in the area of administration” but that “[i]f it is only a private activity without journalistic importance” general data protection interpreted with regard for freedom of expression (c/0.67) would apply. Finally, the Swedish DPA stated that the blog “would fall under the Data Protection Act, but only under a simplified procedure – not the provisions in full” or “could possibly also be exempted” if judged to be done for “journalistic purposes”.⁶⁹



The other two scenarios in this group involved a clear shift in information context, actor and focus (see Table 1). Perhaps related to this, in each case, the DPA responses displayed significant ambiguity as to whether general data protection provisions should be interpreted with regard for freedom of expression (c/0.67) or whether they should simply apply in full (d/1). In the rating website scenario (example 3 – Chart 3 below), almost half of the DPAs (47%) placed the activity within this latter, most stringent category, thereby pushing the

⁶⁹ The answer further clarified that “[t]his exemption should be interpreted extensively and the Supreme Court case law shows that this includes also individuals’ (non-journalists) mentioning of other individuals in their professional capacity for the purpose of discussing society-related issues, even if the information as such is derogatory”.

overall DP engagement score up to 0.8, a result somewhat on the borderline between the two categories.⁷⁰ Whilst there were no free-text answers here, the Polish DPA added to its categorical answer (that general data protection must be interpreted with regard for freedom of expression (c/0.67)) text⁷¹ asserting that, notwithstanding the exclusion of data protection from the face of the e-Commerce Directive 2000/31,⁷² the Polish transposition of this Directive was relevant here. In the case of the social networker (example 4 – Chart 4 below), the modal average pointed to ensuring full application of the provisions (d/1) rather than an interpretation of them with regard for freedom of expression (c/0.67). In contrast, the DP engagement score here (0.71) was very close to the central value of the latter, more liberal interpretative category. This complex outcome was the result of a very wide spread of responses, a diversity which additionally produced by far the highest standard deviation (0.36). Four free-text responses were also received. With the exception of the Swedish response,⁷³ all disclosed a considerable yet still rather ambiguous reluctance to apply data protection law here.⁷⁴ This stance was mirrored by two DPAs (Malta and Slovenia) which combined a standard answer indicating the data protection was inapplicable (a/0) with further text specification.⁷⁵

⁷⁰ Despite the clear clustering of responses into only two categories, this almost even split also resulted in a standard deviation of 0.22, close to the average value.

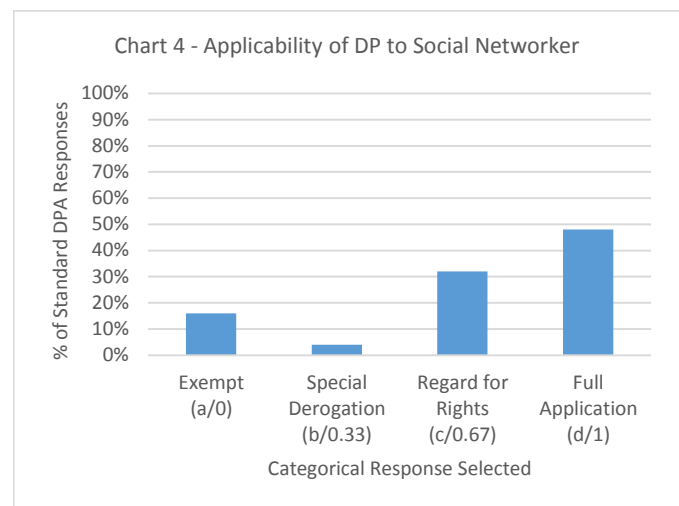
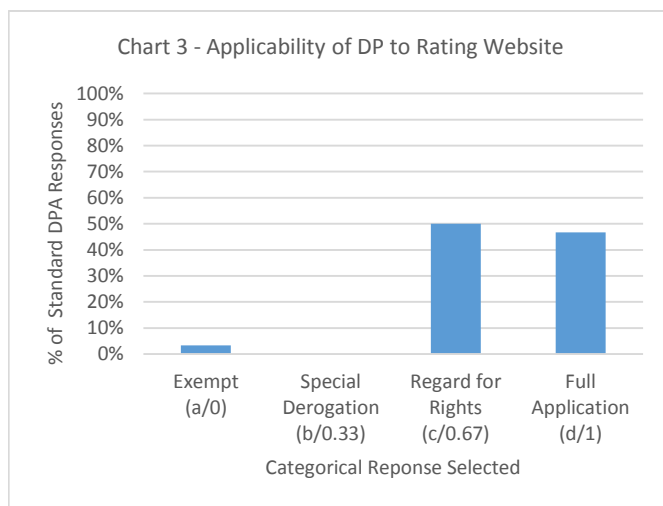
⁷¹ The text stated that “[r]egardless from the above [standard answer], such a case could also be interpreted from the perspective of the Act of 18 July 2002 on providing services by electronic means (Journl of Laws No. 144, item 1204). It would mean that the entity keeping the internet service can interfere in the contents of information entered on the website by service users, if it receives information on their unlawful nature, however, it is not responsible for stored data if it does not know that they have such nature.” In addition, the French DPA combined its category (d/1) answer with a note that “[t]here is case law on this issue in France”. This appears to be a reference to the litigation on the teaching rate website Note2be.com from 2008. See *Note2be.com Ltd, Mr SC v. La Federation Syndicale Unitaire and Others* 08/04727 (Paris Court of Appeal).

⁷² Directive 2001/31, art. 1.5.b (see above).

⁷³ The Swedish response stated that “such publication would fall under the Data Protection Act, but only under a simplified provision – not the provisions in full”, thereby acknowledging that data protection would apply albeit strongly interpreted with regard for various other rights such as freedom of expression.

⁷⁴ Thus, the Finnish DPA responded that “[a]pplication of the Data Protection law (Personal Data Act) depends on the purpose of the tagging”, the Polish DPA stated “[i]n general we consider that the SNS [Social Networking Site] itself is a data controller, and not the individual” whilst the Slovakian DPA held that “Data Protection applies only in the case when a purpose and means of data processing are determined and such activity is performed systematically. If these three conditions are not fulfilled the case of privacy infringement fall within the scope of the Civil Code.”

⁷⁵ The Maltese DPA stated that “[a]pplicability depends on the type of profile and whether this is intended for personal use or for other purposes such as business, or to disseminate specific news or information of a journalistic nature”, whilst the Slovenia DPA noted that “[i]f the member is a data controller, data protection law might apply”.

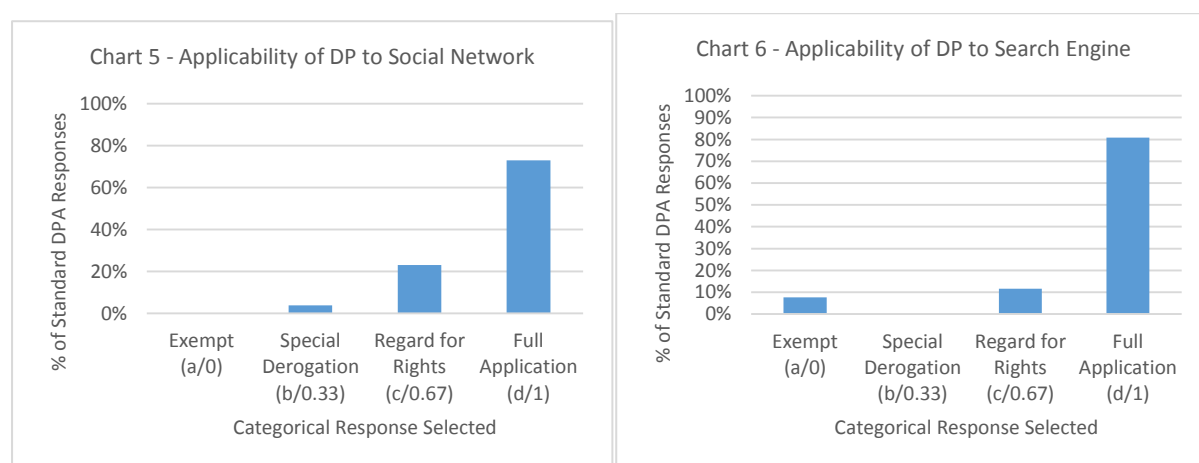


Thirdly, as regards a final grouping of three scenarios (examples five to seven) which involved a corporate social network actor, a search engine and a street mapping service, the DP engagement score clearly indicated a DPAs view that default data protection provisions should be fully applicable (d/1). Notwithstanding the lack of a clear shift in informational context (see Table 1), in the case of the street mapping service publishing photographic images (example 7 – Chart 7 below), this attitude was particularly dominant, thereby resulting in a DP engagement score of 0.98 and an extremely low standard deviation of 0.08. Only a singular free-text response, which indicated a need to interpret and apply data protection with regard for other rights, was received from the Swedish DPA.⁷⁶ In some contrast, as regards the search engine indexing public domain content (example 6 – Chart 6 below), two DPAs (Ireland and Slovakia) held that data protection was entirely inapplicable here (a/0). In addition, three free-text responses were received, two of which declined to disclose a substantive answer.⁷⁷ Overall, however, and notwithstanding the fact that (as Table 1 above again indicates) a generalised search engine clearly at least partially facilitates both the flow of information of collective public interest and information linked to individual self-expression, the DP engagement score remained very high at 0.89. Finally, in the scenario concerning a social networking site processing content originally generated by a user (example 5 – Chart 5 below), a significant number of DPAs (23%) did consider that interpretation with regard for freedom of expression was necessary (c/0.67). Nevertheless, given that a clear majority of DPAs still felt that data protection should apply in full (d/1), the DP engagement score was similarly high at 0.90. Given the clear link between this corporate actor’s activity and the facilitation individual self-expression (cf. Table One), this is also surprising. It may very partially be explained by the fact that, rather than exploring the

⁷⁶ As with the response to the social networker case (example 3), this response stated that “such publication would fall under the Data Protection Act, but only under a simplified provision – not the provisions in full”.

⁷⁷ The Czech DPA stated: “There is no official opinion of the Office on this matter. The Office has not yet encountered the issue”. The Polish DPA noted that a “[s]imilar question is currently under review by the Court of Justice of the European Union, within the C-131/12 Google Spain proceeding. Poland has given its opinion. Since there is no judgment as yet however, we would like to wait with comments. The judgment would likely be decided for interpretation of such cases”. Finally, the Swedish DPA held that “[t]he same conclusion as in the Article 29 Working Party’s opinion on search engines, W148, applies, i.e. the company would be primarily responsible for long term “cache” and value added operations on personal data”.

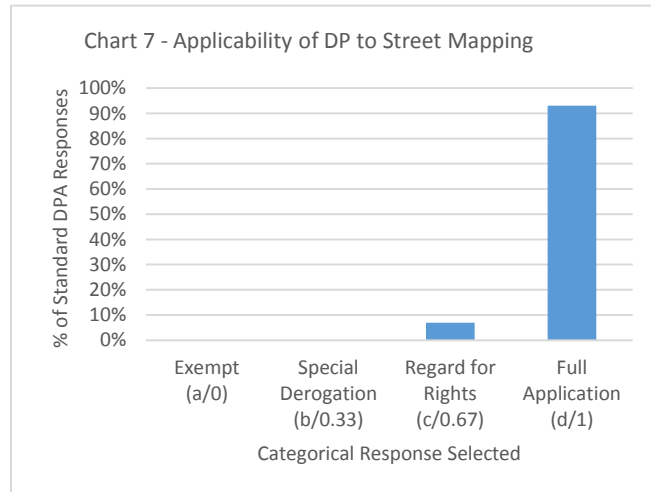
potential *ex ante* responsibilities of such sites to prevent the publication and further processing of inappropriate data (as in the linked case of the social networker in example 4 – Chart 4 above), this scenario only probed the actor’s responsibilities following complaint by a data subject. Such an *ex post* restriction may have been taken by some DPAs to have already balanced default data protection norms with freedom of expression (and related rights) concerns. This hypothesis is bolstered by three⁷⁸ out of the five⁷⁹ specific additional text responses which were forthcoming, all from DPAs which had indicated that data protection was fully applicable (d/1). Three free-text responses were also received here.⁸⁰ Notwithstanding these caveats, however, the responses here clearly indicate that the great majority of DPAs consider that social networking sites such as Facebook have very significant data controller responsibilities even in relation content generated by users.



⁷⁸ Thus, the Cypriot DPA stated “[a]s a rule, a blogger or a social network administrator is not responsible for what visitors write/ publish on his blog/ network. The blogger/ social network administrator IS responsible for dealing with requests for access, rectification and erasure. The blogger/ social network administrator IS responsible to erase data and/ or interrupt the processing of data published on his blog/ network when the Commissioner ascertains, either on his own initiative of following a complaint, that a contravention of the provisions of the Law relating to the application of the basic principles for data processing has occurred (section 4(2) of the DP Law)”. The Maltese DPA stated that “SNS may *remove* content if this breaches the terms and conditions which are wider in scope than Data Protection Rules” (emphasis added). Finally, the Portuguese DPA indicated that “[e]ven considering that the SNS may not be a data controller, it still has some responsibilities concerning the information published, as it is the ‘owner’ of the platform and disseminates the information, and hence it is subject to an order from the DPA to delete the data if considered illegal, despite the liability of the original publisher”.

⁷⁹ The other two DPAs commented as follows. The Bulgarian DPA stated that “[t]he site providing social networking is a personal data controller with regard to the processing of personal data of its users”. Meanwhile, the Slovakian DPA stated “[a]ccording to our national legislation, it is very important for us where the entity is established. If the entity is not established on the territory of the Slovak Republic or means of automatic data processing are not placed on its territory, the case falls within the scope of European data protection legislation but our office cannot act. What we can do is only to send a notice to our partnership DPA and inform a claimant.”

⁸⁰ This Swedish DPA stated that “[b]oth the member of the SNS and the SNS as such could be seen as personal data controllers” and that “such publication would fall under the Data Protection Act, but only under a simplified provision – not the provisions in full”. Meanwhile, the German Länder of Rhineland-Palatinate stated “[f]or this question there are special regulations in the Law of Telemedia and there are high court decisions. If the SNS is expressly informed about the illegal publication, it is responsible and has to delete the illegal content”. Finally, the Liechtenstein DPA noted that “[t]o our understanding, the Social Networking site is not, *prima facie*, a controller. It may be the case, however, under certain circumstances”.



Overall, it is clear that DPAs have generally adopted an expansive understanding of the applicability of default data protection norms to the ‘new media’. If all seven of the ‘new media’ scenarios are considered together, then it can be seen that no fewer than 93% of the standard responses received held that the activity in question fell, in principle, within the scope of data protection law (by coming within categories b/0.33, c/0.67 or d/1). Even more strikingly, only 11% of the responses across these scenarios held that the special purposes derogation (b/0.33) was engaged. More, whilst the overall median DP engagement score (0.75) was closest to category (c/0.67), thereby suggesting a general need to interpret general data protection provisions with regard for freedom of expression (and related rights) in the new media context, the modal response and indeed a bare majority of all standard responses indicated that such provisions should simply apply in full (d/1). At the same time, the results also highlight very significant diversity between the DPAs. Not only was the overall standard deviation 0.23 but, even more strikingly, in relation to all but two of the scenarios, at least one and sometimes several standard responses were located at both the extremes of finding data protection totally inapplicable (a/0) and applicable in full (d/1).

Further Analysis

The results elucidated above clearly raise a large number of issues which warrant further analysis. The most pressing of these will be explored below. To begin with, there is a possible relationship between differences in DPA response and divergence in the way in which Directive 95/46 has been transposed in the various EEA jurisdictions. This issue will be explored first. Secondly, the compatibility of the DPA stances with binding CJEU jurisprudence must be considered. Finally, the article will both evaluate the normative appeal of the stances of the DPAs and explore how they might, and should, be subject to modification in the context of the proposed reform of European data protection law.

DPA responses and national data protection law divergence

It may be hypothesised that the different DPA responses may be related to divergences in the transposition of Directive 95/46. As outlined near the beginning of this article, the only part of this Directive explicitly designed to regulated aspects of the relationship between “[p]rocessing of personal data and freedom of expression” is the special purposes provision found in Article 9. As also briefly noted there and explored further below, EEA jurisdictions have interpreted the *scope* of this provision rather differently. The formal *depth* of the derogation for the special purposes set out in national law also diverges widely. This reality has been exhaustively captured by this author elsewhere through quantitatively coding the continuing applicability in formal national data protection law of default substantive data processing standards in the area of institutional journalism on scale ranging from 0 (a full substantive derogation) through to 1 (the complete substantive applicability of default data protection).⁸¹ In addition, it could be argued that the transposition of the second intent of Article 3.2 of the Directive, which entirely excludes certain personal and household activity from data protection, might also be relevant at least as regards some ‘new media’ activity carried out by individuals. However, in this case, in light of the strong principle of harmonious interpretation or indirect effect,⁸² transposition divergences are so minor that they would not generally lead to a result different from the binding CJEU decision in *Lindqvist* which, as noted above, held that this exemption could not cover “processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people”.⁸³ The definition of ‘new media’ utilized in this article is expressly confined to instances of indefinite publication.

Turning to divergences in the *scope* of the special purposes within national legislation, EEA jurisdictions can be ordered into five classes which range from the narrowest through to the broadest conceptualisation of the type of activities which should be shielded from general data protection norms in this way. These five categories are as follows:

- **Class (i) (No derogation):** Firstly, three jurisdictions (Croatia, Czech Republic and Spain) fail to provide for a special derogation for any expressive purposes and, therefore, *ipso facto* have the narrowest approach to these provisions possible.
- **Class (ii) (Institutional media derogation):** Next, six jurisdictions (Austria, Estonia, Germany, Hungary, Liechtenstein and Slovenia) limit this derogation to the protection of the media only.⁸⁴

⁸¹ D. Erdos, “European Union Data Protection Law and Media Expression: Fundamentally Off Balance” (2015) 64 *ICLQ* (forthcoming). Although this article specifically focuses on the derogation as applicable to the institutional journalism, in the great majority of cases its depth is identical as regards other specially protected expressive purposes such as literature and art.

⁸² *Marleasing SA v La Comercial Internacional de Alimentacion SA* (C-106/89) EU:C:1990:395.

⁸³ *Lindqvist* (C-101/01) EU:C:2003:596 at [47]. In only three jurisdictions is the situation, arguably, less clear-cut. Irish law excludes not only “personal data kept by an individual and concerned only with the management of his personal, family or household affairs” but also data “kept by an individual only for recreational purposes”. See Ireland, *Data Protection Acts*, s. 1 (4) (c). Somewhat similarly, United Kingdom law exempts data “processed by an individual only for the purposes of that individual’s personal, family or household affairs (including recreational purposes)”. See UK, *Data Protection Act*, s. 36. Finally, although one provision within Polish law expressly excludes processing of data by natural persons “for personal or domestic purposes exclusively”, another states that the legislation applies *inter alia* to “natural and legal persons and organizational units not being legal persons, if they are involved in the processing of personal data as part of their business or professional activity or the implementation of statutory objectives”, a phrasing which could imply that all non-business, professional or official activity by both natural and legal persons is outside the scope of this law. See Poland, *Act on the Protection of Personal Data*, art. 3 (a) (1) and art. 3 (2) (2).

⁸⁴ Austria, *Federal Act concerning the Protection of Personal Data (DSG)*, s. 48; Estonia, *Personal Data Protection Act*, art. 11 (2); Germany, *Federal Data Protection Act*, s. 41 (2); Hungary, *Act on Informational Self-Determination and Freedom of Information*, s. 65(3)(g); Liechtenstein, *Data Protection Act*, art. 1.3 & 17.2 and Slovenia, *Personal Data Protection Act*, art. 7 (3).

Although each law's definition of 'the media' differs in certain respects, they are in all cases suggestive of not only a purpose specific but also an institution specific provision, thereby encapsulating the understanding in the original draft of the Directive produced by the European Commission in 1990, which limited the derogation to processing in respect of the press and the audiovisual media.

- **Class (iii) (Journalism and/or art derogation):** Three further jurisdictions (Cyprus, Greece and Italy) set out an entirely purpose, as opposed to actor, specific derogation, but make this narrower in scope than the maximum set out in Article 9 itself. Greece limits the derogation to "journalistic purposes",⁸⁵ whilst Cyprus⁸⁶ and Italy⁸⁷ protects not only journalistic purposes but also artistic expression.
- **Class (iv) (Journalism, literature and art derogation):** Next, a fourth category of some fifteen - that is almost half of - EEA jurisdictions set out a special purposes provision which is generally as broad, but no broader, than the scope of Article 9 of the Directive itself. These jurisdictions are Belgium, Bulgaria, Finland, France, Gibraltar, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia and the United Kingdom.⁸⁸
- **Class (v) (Supra journalism, literature and art derogation):** Finally, four jurisdictions (Denmark, Iceland, Malta and Sweden) provide for a special purpose shield which is broader than that set out on the face of Article 9 itself. However, the extent of this broadening is very different in each case. In addition to generally shielding all data "solely processed in the interests of journalism or a literary and artistic activity", Article 6 of the Icelandic *Data Protection Act* also states that "[t]o the extent that it is necessary to reconcile the right to privacy on the hand with the freedom of expression on the other, derogations can be made from the provisions of the Act in the interest of journalism, literature and art", a wording that is clearly somewhat wider than Article 9 alone.⁸⁹ Section 6 of the Maltese *Data Protection Act* makes no mention of literary or artistic expression but rather provides a partial shield for "freedom of expression" as set out in the Maltese *European Convention Act*, as well as shielding "the provisions of the Press Act relating to journalistic freedoms". Meanwhile, the Danish *Data Protection Act* not only sets out derogations for the purposes of journalism, artistic or literary expression,⁹⁰ but also states that the law "shall not apply where this will be in violation of the freedom of information and expression, cf. Article

⁸⁵ Greece, *Data Protection Act*, art. 7 (2) (g) and art. 11 (5). Art. 7 (2) (g) does appear to link "journalistic purposes" not only to provision of "information on matters of public interest" but also to engaging in "literary expression". However, this suggestive language does not detract from the fact that the gateway for any exemption remains being engaged in "journalistic purposes".

⁸⁶ Cyprus, *Processing of Personal Data (Protection of Individuals) Law*, s. 6 (1) (i).

⁸⁷ Italy, *Personal Data Protection Code*, s. 136 (1).

⁸⁸ Belgium, *Act on the Protection of Privacy in Relation to the Processing of Personal Data*, s. 3; Bulgaria, *Law for the Protection of Personal Data*, art. 4 (7); Finland, *Personal Data Act*, s. 2 (5); France, *Law on Information Technology and Liberties*, s. 2 (5); Gibraltar, *Data Protection Act*, s. 13 (1); Ireland, *Data Protection Acts*, s. 22A; Latvia, *Personal Data Protection Law*, art. 5 (1); Lithuania, *Law on Legal Protection of Personal Data*, art. 8; Luxembourg, *Law on the Protection of Persons with Regard to the Processing of Personal Data*, art. 9; Netherlands, *Personal Data Protection Act*, art. 3 (1); Norway, *Personal Data Act*, s. 7; Poland, *Act on the Protection of Personal Data*, art. 3a; Portugal, *Act on the Protection of Personal Data*, art. 10 (6) and 11; Romania, *Law on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data*, art. 11; Slovakia, *Act on the Protection of Personal Data*, s. 7 (4) (a) and s. 10 (3) (d) and the United Kingdom, *Data Protection Act*, s. 3.

⁸⁹ It is difficult, albeit not impossible, to decipher what processing might be "in the interests of journalism, literature and art" but not solely so. One example might be disclosing for publication data which is clearly being held for a divergent purpose.

⁹⁰ Denmark, *Compiled Version of the Act on Processing of Personal Data*, s. 2 (6) and s. 2 (10).

10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms”.⁹¹ Finally, the Swedish *Personal Data Act* goes by far the furthest in disapplying data protection in the interests of freedom of expression. Beyond setting out an unconditional exemption from the substantive data protection provisions for processing for journalistic purposes and for the purposes of artistic or literary expression,⁹² the Swedish Act also states that its provisions “are not applied to the extent that they would contravene the provisions concerning ... freedom of expression contained in ... the [Swedish] Fundamental Law on Freedom of Expression”.⁹³ This Fundamental Law provides for a right to publicly “communicate information on any subject whatsoever” including through “public playback of material from a database”⁹⁴ as well as “to procure information on any subject whatsoever for such communication or publication”.⁹⁵ There is no requirement that this dissemination fall within the definition of journalism, literary or artistic expression; to the contrary, a database is simply defined as “a collection of information stored for automatic data processing”.⁹⁶

Similarly to the standard responses to the DPA survey, it is possible to transpose these special purpose scope classes into special purpose scope scores through transposing them onto a 0, 1 scale. In this way, class (i) becomes equal to 0, (ii) to 0.25, (iii) to 0.5, (iv) to 0.75 and (v) to 1. In contrast to the DPA survey new media scenario scores, the *lowest* score here (i/0) represents the most *stringent* DP approach (namely no special purposes derogation) and the *highest* score (v/1) the most *deregulatory* one (namely a derogation which extends beyond the wording found in Directive 95/46 itself).

In principle, it is possible that there might be a *direct* and/or *indirect* relationship between the scope of the special purposes within national law and the DPA stance as regards the new media. Given this, two new variables were construed. (In the construction of both these variables, missing standard responses from DPAs were addressed by imputing the nearest standard response based on an analysis of their free-text answer or, in the two cases where no substantive free-text answer was provided, the answer given by the overwhelming majority of the other DPAs.)⁹⁷ Turning to the possibility of a *direct* relationship, it may be hypothesized that a wide statutory construction of the special purposes will lead DPAs to be more ready to find that new media activity itself falls within this provision. Therefore, a simple count was made of the number of times each DPA had held (or had been imputed to hold) the special purposes derogation to be itself applicable to the various scenarios outlined. In this case, a *high* value for both the special purposes scope score and this count value indicates a more *deregulatory* approach. Therefore we should expect a positive and significant correlation here. In fact, the correlations run were clearly insignificant (and in a different to expected direction).⁹⁸ It may,

⁹¹ Ibid, s. 2 (2).

⁹² Sweden, *Data Protection Act*, s. 7.

⁹³ Ibid.

⁹⁴ Sweden, *Fundamental Law on Freedom of Expression*, art. 1.

⁹⁵ Sweden, *Data Protection Act*, s. 2.

⁹⁶ Ibid, art. 1.

⁹⁷ The Slovenian free-text response to scenarios 0, 1 and 2 was considered to be a clear admixture of both a/0 and d/1. As a result an average was taken of these, resulting in a unique score of 0.5. Given that the Netherlands DPA had not provided any kind of answer to five out of the seven new media examples it was decided that it was not practicable to impute missing values in this case.

⁹⁸ The Pearson correlation was - 0.089 with a (two-tailed) significance value of 0.648. Meanwhile, the Spearman’s rho correlation was - 0.028 with a (two-tailed) significance value of 0.883.

however, still be hypothesized that an *indirect* relationship is possible. In such a scenario, whilst not finding new media activity itself to fall within the special purposes, a DPA operating within a jurisdiction with a broad special purposes derogation might nevertheless be swayed by this deregulatory approach to find general data protection provisions less engaged, for example, by holding that vis-à-vis the new media, data protection provisions must be interpreted with regard for freedom of expression (c/0.67) rather than simply being applicable in full (d/1)). To explore this possibility, an overall new media DP engagement score was constructed as an average of the numerical cognate to the categorical scores the DPA had provided (or been to imputed to provide) in relation to all seven new media scenarios. (The values calculated here are listed in the appendix at the end of this article). In contrast to the special purposes scope measure, a *high* score here (closest to the d/1 category) represents a *stringent* approach and a *lower* score (closest to the a/0 category) a more *deregulatory* one. We should therefore expect a significant and negative relationship here. The results indicate some support for this hypothesis. Both measures of correlation show a clear negative relationship, with (two-tailed) significance at the 0.1 level.⁹⁹

This author's quantitative measure of the continued formal applicability of default data protection even in the area of institutional journalism (which focuses not on the *scope* but the *depth* of the special purposes derogation) was also correlated with, firstly, a count of the number of times the special purposes derogation was itself found applicable to new media activity and, secondly, the overall new media DP engagement score. In general, a more stringent approach within the formal law might reasonably be associated also with a more stringent regulatory approach. If so, we should expect a significant negative correlation in the first case and positive correlation in the second. In this case, both results bore out these hypotheses with (two-tailed) significance either at the 0.05 or the 0.1 level. In sum, DPAs operating in jurisdictions whose formal laws apply substantive data protection provisions strongly even within the special purposes area, also appear less likely to find that new media activity falls within these protected purposes¹⁰⁰ and additionally adopt a more stringent interpretative approach in the wider new media setting as well.¹⁰¹ Thus, notwithstanding that their explicit ambit is clearly restricted and in the view of most DPAs not directly engaged by most new media activity,¹⁰² the attitude of Member State law as to the permissibility of derogations from data protection *within* the special purposes appears to capture broader divergence, also shared by the national DPAs themselves, as to the extent to which data protection should give way to public freedom of expression more widely.

DPA Responses and Pan-European CJEU Interpretations

Notwithstanding the interesting correlations detailed above, there is no direct relationship between specific provisions in national data protection law and the interpretative stance adopted by the DPAs in the new media context (as outlined in Table 2 above). This, in turn, makes it particularly important to consider whether

⁹⁹ The Pearson correlation was - 0.351 with a (two-tailed) significance value of 0.062. Meanwhile, the Spearman's rho correlation was - 0.314 with a (two-tailed) significance value of 0.097.

¹⁰⁰ The Pearson correlation was - 0.399 with a (two-tailed) significance value of 0.032. Meanwhile, the Spearman's rho correlation was - 0.387 with a (two-tailed) significance value of 0.038.

¹⁰¹ The Pearson correlation was 0.349 with a (two-tailed) significance value of 0.063. Meanwhile, the Spearman's rho was 0.342 with a (two-tailed) significance value of 0.069.

¹⁰² As Table 2 above indicates, overall, 89% of the standard responses to the new media scenarios presented did not consider the special purposes provision to be applicable.

these stances are consistent with binding pan-European CJEU legal interpretations. Given its seminal importance, *Google Spain*¹⁰³ cannot be excluded from this analysis. At the same time, it should be emphasised that this decision had not been handed down by the time the responses to the survey analysed in this article had been completed.¹⁰⁴

CJEU case law in this area was briefly outlined near the beginning of this article. As explored there, the CJEU has continuously stressed - most notably in *Lindqvist* and *Satamedia* - that exemptions from data protection must be construed narrowly and, in any case, cannot cover publication of information to an indefinite number. These judgments would, therefore, appear to be in conflict with the, albeit small, number of DPAs which held various new media activities to be entirely exempt from data protection requirements. More ambiguous is the relationship between CJEU jurisprudence and the general reluctance of DPAs to find the special purposes derogation applicable as regards most forms of new media communication. This might appear to be in clear conflict with the finding in *Satamedia* that the phrase “solely for journalistic purposes” could cover all activities whose “sole object ... is the dissemination to the public of information, opinions or ideas”.¹⁰⁵ However, whilst some have argued this definition was “tantamount to declaring that all expression must be classified as such [solely journalistic]”,¹⁰⁶ this is an overbroad reading of the case. Read contextually, the Court was protecting only those activities objectively orientated to communicating material to ‘the public’ conceived as a collective grouping (akin to the *body politic*) rather than simply the communication to any indefinite group of persons. Thus, the judgment made no attempt to distance itself from *Lindqvist* where, as previously noted, the Court refused to accept the Commission’s claim that the website in question fell within the special purposes.¹⁰⁷ Moreover, in *Google Spain*, the Court made explicit its understanding that the making available of public domain material by a general search engine could not be deemed a special purpose.¹⁰⁸ Given this, the general DPA stance that the new media activities outlined in scenarios three to seven of the survey fall outside the special purposes derogation is probably legally sound. As Table 1 outlined, these activities are not predominantly linked to disseminating material of collective public interest. The modal understanding of DPAs that a media archive (example 1) does not lose special purposes protection also appears legally tenable so long as any such service remains orientated to serving the public collectively (by, for example, helping facilitating ongoing public debate) rather than serving particular private interests.¹⁰⁹ Far more problematic, however, is the exclusion by many DPAs of amateur bloggers such as that outlined in example two from this special shield. Similarly to the traditional media, the blogger here was seeking to disseminate material which is widely claimed

¹⁰³ *Google Spain* (C-131/12) EU:C:2014:317.

¹⁰⁴ The final judgment in this case was not released by the Court until 13 May 2014. Meanwhile, the Advocate General’s Opinion, which adopted a very different interpretation of EU data protection law, was published on 25 June 2013 (Opinion in *Google Spain*, *Google v Agencia Espanola de Proteccion de Datos*, *Mario Coseja Gonzales* (C-131/12) EU:C:2013:424). This was after responses had been received back from all but three of the DPAs (Bulgaria, Cyprus and Liechtenstein).

¹⁰⁵ *Satamedia* (C073.07) EU:C:2008:727 at [61]. As outlined in note 48, this definition was in principle limited to processing “relating to documents which are in the public domain under national legislation” [Ibid].

¹⁰⁶ Oliver, “The protection of privacy in the economic sphere before the European Court of Justice”, p. 1454.

¹⁰⁷ *Lindqvist* (C-101/01) EU:C:2003:596 at [33].

¹⁰⁸ *Google Spain* (C-131/12) EU:C:2014:317 at [85]. For an extended analysis of case law on this point see D. Erdos, “From the Scylla of Restriction to the Charybdis of License? Exploring the Scope of the ‘Special Purposes’ Freedom of Expression Shield in European Data Protection” (2015) 52 *CMLR* 119.

¹⁰⁹ Whether a public orientation remains will very much depend on the circumstances. Whilst most forms of free online news archives, such as that set out in example 1 of the survey, would appear to be so orientated, this would clearly not be the case for services which use news archives in a way specifically tailored to facilitate purely private purposes. One such example is the Know Your Candidate’s Adverse Media Check which “enables employers to search a vast array of media sources quickly for articles linking their candidate to crime or terrorism” (Know Your Candidate, *Adverse Media Check* (n.d.) <http://www.knowyourcandidate.co.uk/adverse-media-check.cfm> [accessed May 16, 2015].

to be of legitimate interest to the collective public.¹¹⁰ The apparently institutionally restricted understanding of the special purposes adopted by these DPAs is profoundly at odds with the emphasis in *Satamedia* that “journalistic purposes” were “not limited to media undertakings”¹¹¹ but, rather, instantiated an aspect of freedom of expression enjoyed by everyone.¹¹² In any case, Article 9 on its face protects “literary and artistic expression”, a phrasing which is self-evidently broader than professional journalistic activity alone.

As regards DPAs’ conceptualization of the second grouping, where a rounding of the average DP engagement score pointed to recognition that general data protection provisions apply but must nevertheless be interpreted with regard for freedom of expression, the key case to consider is *Lindqvist*. Here, the Court suggested that as regards the type of internet activity engaged in by Mrs Lindqvist, there was an obligation to have regard for freedom of expression. Although there are some major disjunctures between Mrs Lindqvist’s internet page and the social networker and rating website scenarios detailed in examples three and four of the survey, they all share a predominant link to individual self-expression (see Table 1). Given this, those DPAs which did recognise a need to have regard for freedom of expression in these examples would appear to be acting most consistently with CJEU case law.

In the third grouping which comprised the corporate social networking site, search engine indexer and street mapping service (examples 5 to 7), the majority of DPAs clearly held that general data protection provisions should be applicable in full, apparently without any to expressly take freedom of expression into account. In *Google Spain*, the CJEU indicated that neither the dissemination of personal information for reasons of “economic interest” nor the “interest of the general public” in receiving such information triggered a requirement to explicitly interpret data protection with regard for freedom of expression.¹¹³ A street mapping service (example 7) would appear to provide an example of just such an essentially private “service”.¹¹⁴ Rather surprisingly, however, the *Google Spain* judgment also appeared to conceptualize indexing by a generalized search engine (example 6) in a like manner. This is despite the fact that such activity also plays a key role in facilitating both individual self-expression and communication of collective public interest (see Table 1). Nevertheless, certain aspects of the judgment sit in tension with its general tenor. Firstly, despite explicitly rejecting Google’s allegations of a violation of the principle of proportionality¹¹⁵ and holding it to be a data controller,¹¹⁶ the Court argued it would only have data protection duties “inasmuch” as its activity is “liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data” and, even then, only needed to act within the framework of its “responsibilities, powers and capabilities”.¹¹⁷ Such wide limitations of legal duty are nowhere found within

¹¹⁰ Even if the legitimacy of such information flow is (perhaps rightly) questioned, this should be addressed by limitations within the special purposes derogation rather than placing such substantive types of dissemination outside it. In this context, it should be noted that the CJEU in *Satamedia* was emphatic that the derogations provided even for the special purposes “must apply only in so far as is strictly necessary” to achieve a balance between fundamental rights (at [56]).

¹¹¹ *Satamedia* at [61].

¹¹² Such an understanding is also in tension with the Article 29 Working Party of EU DPAs’ own Recommendation 1/97 on *Data Protection Law and the Media* which also argued that “Article 9 of the directive respects the right of individuals to freedom of expression. Derogations and exemptions under article 9 cannot be granted to the media or to journalists as such, but only to anybody processing data for journalistic purposes” (Article 29 Working Party, *Recommendation 1/97 Data Protection Law and the Media* (1997), p. 8, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp1_en.pdf [accessed May 16, 2015]).

¹¹³ *Google Spain* (C-131/12) EU:C:2014:317 at [97].

¹¹⁴ *Ibid* at [55].

¹¹⁵ *Ibid* at [63].

¹¹⁶ *Ibid* at [34].

¹¹⁷ *Ibid* at [38].

Directive 95/46 itself. Secondly, although stressing that in other respects search engines must “ensure ... that the activity meets the requirements of Directive 95/46”,¹¹⁸ the Court did not explicitly stipulate that search engines had to adhere to the very onerous rules applicable to the processing of sensitive information under Article 8. Thirdly, whilst the Court held that data subjects would “as a rule” have the right to demand that even ordinary personal data be removed from search engine results linked to their name, it did acknowledge that “that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question”.¹¹⁹ It may be that subsequent CJEU case law will extend this public interest test to sensitive classes of data, an expansion which would clearly entail recognition of need to interpret the law with regard for the right of the public to receive information in this form, an aspect of freedom of expression. Thus, whilst the legal understandings of DPAs that street mapping services must adhere to general data protection provisions in full is clearly based on established legal principle, the situation as regards search engines is much more unstable.¹²⁰ Finally, the majority understanding of DPAs as regards the social networking site scenario (example 5) appears to be at least as legally questionable. In so far as this corporate actor is simply enabling individuals to publish and ‘tag’ images of identified persons, it shares a similar and still critical link to individual self-expression as the activity of the social networkers themselves (example 4). Therefore, the logic of *Lindqvist* would appear to point to a need to interpret general data protection provisions with regard for freedom of expression here.¹²¹

Evaluation

In granting general data protection provisions an expansive role in the area of new media communications, the general interpretative stance of DPAs raises a number of concerns, especially as regards freedom of expression. Firstly, the reluctance of many DPAs to extend the special purposes shield beyond cases of institutional publishing, thereby removing amateur bloggers from this shield, is not only contrary with the ratio of *Satamedia* but more fundamentally conflicts with the liberal democratic notion that journalism (and

¹¹⁸ Ibid at [38].

¹¹⁹ Ibid at [97].

¹²⁰ It is notable that, in some contrast to both *Google Spain* and the tenor of the DPA responses, the Article 29 Working Party Group of EU DPAs have recently acknowledged that a particular type of regard must be had to freedom of expression in the case of search engines. In sum, it stated “[t]he interests of search engines in processing personal data is economic. But there is also an interest of internet users in receiving the information using the search engines. In that sense, the fundamental right of freedom of expression, understood as ‘the freedom to receive and impart information and ideas’ in Article 11 of the European Charter of Fundamental Rights, has to be taken into consideration when assessing data subjects’ requests [to have material deindexed against their name]” (Article 29 Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González”* C-131/12, p. 6, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf [accessed May 15, 2015]). This perspective also chimes with an earlier 2008 statement of the Working Party that it was “aware of the special role search engines have in the online information environment” and that “[a] balance needs to be struck by Community data protection law and the laws of the various Member States between the protection of the right to private life and the protection of personal data on the one hand and the free flow of information and the fundamental right to freedom of expression on the other hand” (Article 29 Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, p. 13, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [accessed May 16, 2015]).

¹²¹ It may well be that the social networking site uses such ‘tagged’ data not only to facilitating individual self-expression but also for other purposes such as commodifying the data and even using it to track the tagged person around the internet. CJEU jurisprudence would point to a need to apply general data protection in full as regards these latter purposes. Nevertheless, it would still seem important to be able to ‘granularize’ the processing such the activity which was purely orientated to facilitating self-expression continued to benefit from an interpretation which had express regard for freedom of expression rights.

other forms of professional writing) are simply “the exercise by occupation of the right to free expression available to every citizen”.¹²² Secondly, in a complex digital environment, the best reading of *Lindqvist* correctly points to the need to take freedom of expression into account not only vis-à-vis individuals themselves but also as regards any service provided by corporate actors which is limited to the facilitation of such self-expression. At least as regards social networking sites, however, this necessity appears to not to have been fully accepted by the majority of DPAs. Although other aspects of DPAs’ general approach are generally consistent with CJEU jurisprudence, this case law itself is far from being normatively unproblematic. Thus, the suggestion in *Lindqvist* that, as regards activities strongly linked to individual self-expression, general data protection provisions should simply be interpreted with regard for freedom of expression sits in tension with the need for limitations on fundamental rights to be “provided for by law” (as per the EU Charter)¹²³ or “prescribed by law” (as per the European Convention).¹²⁴ In addition, the focus of the CJEU on interpretation renders opaque whether such efforts by national courts and DPAs should lead to whole aspects of national data protection law (for example, the rules as regards sensitive information) being disregarded in certain circumstances, or whether (in the absence of a specific and optional derogations made under Art. 13 (g) or Arts. 8.4 - 8.5 of Directive 95/46) only a particular gloss may be given to less fundamental or already open-textured¹²⁵ aspects of the legal regime. Even more starkly, the failure by the CJEU in *Google Spain* to acknowledge that the regulation of a search engine’s public indexing function engaged freedom of expression at all has been subject to vigorous and telling criticism. For example, Kulk and Borgesius argue that the CJEU judgment “suggests that privacy and data protection rights override, ‘as a rule’, the public’s right to receive information (referred to as an ‘interest’ rather than a right by the CJEU). That ‘rule’ is an unfortunate departure from the doctrine developed by the European Court of Human Rights”.¹²⁶ They also note the rather alarming reality that “after the decision, it seems that in some situations search engine operators do not have a legal basis for indexing websites that contain special [sensitive] categories of data. In principle, a search engine operator would need the data subject’s explicit consent for indexing pages that include special categories of data. Such a requirement would render the activities of a search engine operator practically impossible”.¹²⁷ Finally, the serious diversity in the DPA responses must also be considered. This diversity is exemplified in the fact that, in relation all but two of the new media scenarios, at least one DPA understood the activity in question to be entirely exempt from data protection (category a/0), whilst at least one other considered the general provisions of data protection to be applicable in full (category d/1) (see Table 2). Such wide divergence raises concern about the integrity of the European data protection regime. This legal framework is expressly designed to ensure that, as regards the processing of personal data, “the level of protection of the rights and freedoms of individuals ... be equivalent”.¹²⁸ It is this equivalency which justifies Member States’ obligation to ensure both the free flow of such data across the EEA¹²⁹ and, so long as data processing is only taking place within the context of an establishment in another Member State, the non-application of their own data protection law to the controller’s

¹²² G. Robinson, *People Against the Press: An Enquiry into the Press Council* (London: Quartet Books, 1983), p. 3.

¹²³ EU Charter, art. 52.

¹²⁴ European Convention, art. 10.

¹²⁵ For example, the obligation to process data ‘fairly’ as set out in art. 6 (1) (a), Directive 95/46.

¹²⁶ S. Kulk and F. Borgesius, “Google Spain v. González: Did the Court Forget about Freedom of Expression?” (2014) 3 *European Journal of Risk Regulation* 389.

¹²⁷ *Ibid.*

¹²⁸ Directive 95/46, recital 8.

¹²⁹ Directive 95/46, art. 1.1.

activities.¹³⁰ In fact, the evidence amassed through the DPA survey would suggest that the alleged equivalency of legal approach is completely illusory as regards many activities of the new media.

Reform

In January 2012 the European Commission proposed replacing Directive 95/46 with a new Data Protection Regulation.¹³¹ As the Commission's accompanying Communication stated, this proposal primarily seeks to address two current failures, namely, that the "existing rules provide neither the degree of harmonisation required, nor the necessary efficiency to ensure the right to personal data protection".¹³² As regards the interaction between data protection and freedom of expression, however, the Commission's proposal suggested almost no change. Article 80 of its draft Regulation, which would replace Article 9 of the current Directive, maintained the reference to processing "carried out solely for journalistic purposes or the purpose of artistic or literary expression"; meanwhile, a new recital simply endorsed and amplified the relatively broad interpretation of this phrase adopted by the CJEU in *Satamedia*, clarifying in the process that this provision should cover "news archives and press libraries".¹³³ In contrast, the European Parliament's legislative resolution of March 2014 was much more radical, proposing that Article 80 should be reworded so as to mandate and require Member States to provide for "derogations ... whenever this is necessary in order to reconcile the right to the protection of personal data with the rules governing freedom of expression in accordance with the Charter of Fundamental Rights of the European Union".¹³⁴

Given that all of European data protection is intrinsically in tension with freedom of expression,¹³⁵ this expansive wording could in principle translate the entirety of this extremely discretionary special purposes shield into a provision of universal application, thereby both undergirding and exacerbating the absence of data protection equivalency identified in this article.¹³⁶ However, especially since such a radical expansion of national autonomy would strongly conflict with core harmonizing purpose of the proposed Regulation, legal interpretation of this clause would likely seek to restrict it primarily or even entirely to activities aiming at or

¹³⁰ Ibid, art. 4(1)(a).

¹³¹ European Commission, *op. cit.* supra note 9.

¹³² European Commission, *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century* (COM (2012) 9 final), p. 3.

¹³³ European Commission, *op. cit.* supra note 9, recital 121.

¹³⁴ European Parliament, *Legislative Resolution of 12 March on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, amendment 189, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> [Accessed May 16, 2015].

¹³⁵ As Fritz Hondius, then Deputy to the Director of Human Rights for the Council of Europe stated as far back as 1983 "Data Protection is not so much a set of rules concerning privacy (Article 8 of the [European] Human Rights Convention) as a set of restrictions on the exercise of freedom of information (Article 10) in the interest of the protection of other rights and freedoms (including the right to privacy)." (F. Hondius, 'A Decade of International Data Protection' (1983) 32 *NILR* 103, p. 114).

¹³⁶ It may be argued that the suggested expansion of the so-called household exemption from data protection (currently set out in art. 3.2) would also affect some rebalancing of this tension. In particular, although the Commission's original draft suggested no alteration to the *status quo* here, the Council's compromise text has now proposed excluding all activity "by a natural person ... in the course of ... a personal or household activity" (art. 2 (2) (d)), whilst also clarifying that such activities "include social networking and on-line activity undertaken within the context of such personal and household activities" (recital 15) (Council of the EU, *Annex to Note from the Presidency to Council*, 9565/15 (11 June 2015) <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> [accessed June 26, 2015]). However, such rewording would not only have no effect on activities pursued otherwise than by a non-commercial natural person but, given that the exemption would still be tied to personal or household activity (which the CJEU in *Lindqvist* interpreted as excluding indefinite publication), would probably not significantly effect the legal situation governing mass communication by such a sole individual.

instantiating the disclosure to the public of information, opinions and ideas.¹³⁷ In sum, therefore, an unsustainable degree of ambiguity would appear to haunt the Parliament's proposed new wording.

Seemingly in recognition of drawbacks in both the Commission's and the Parliament's preferred text, the Council of the EU's compromise text agreed on 15 June 2015 included a new bifurcated version of Article 80 which stated:

1. The national law of the Member State shall reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.
2. For the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from the provisions in Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (co-operation and consistency) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.¹³⁸

Whilst clearly an advance on the previous versions of this Article, this proposal still poses a number of difficulties. Firstly, the definition of the special purposes, which rightly benefits from the widest and deepest derogation via Article 80.2, draws an unhelpful distinction between "journalistic purposes" and other forms of the special purposes which are defined in a seemingly more circumscribed fashion as "academic, artistic or literary expression". Given the current regulatory *zeitgeist*, this phrasing still has the potential to encourage an unwarranted prioritization of institutionalized journalism which, as the evidence above indicates, is a serious current problem. Given this, it would be preferable to simply refer equally to academic, artistic, journalistic and literary expression¹³⁹ or even, following on from the logic of *Satamedia*, replace the reference to journalism with the rather broader phraseology of "all activities which aim or instantiate disclosure to the public of information, opinions or ideas".¹⁴⁰ Secondly, although Article 80.1 rightly recognises that certain aspects of freedom of expression outside these special purposes are also worthy of particular shielding, it fails to provide any specification of the forms of expression likely to fall within this or elucidate the nature of the reconciliation intended. Presumably, given that Article 80.1 itself grants no new powers to Member States, it can only operate as an instruction that they should ensure that such a reconciliation is provided for through the various parts of the Regulation which do grant them such discretion. Critical here are the derogatory provisions set out in Article 21 (applicable to many of the ordinary default data protection requirements) and Article 9 (2) (applicable to the sensitive data rules), themselves largely the cognate of Article 12 and Article 8 (4) – (5) of the current Directive. It is vital that the wording of these provisions remain flexible enough to enable Member States to

¹³⁷ Such a limitation is hinted at in a recital of the European Parliament's Legislative Resolution which states that "[i]n order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom broadly *to cover all activities which aim at the disclosure to the public of information, opinion or ideas*, irrespective of the medium which is used to transmit them, also taking into account technological development" (European Parliament (supra note 134), recital 121) (emphasis added).

¹³⁸ Council of the EU (supra 136).

¹³⁹ As, in fact, is the case in Recital 121 of the Council's new draft (ibid).

¹⁴⁰ For a full discussion of this latter point see Erdos (supra 108).

effect an appropriate balance here. In addition, it would be helpful to set out in recitals, firstly, the particular forms of non-special purpose expression which are particularly likely to require derogatory treatment (notably those which instantiate individual self-expression (such as in examples three to five) and those which facilitate both individual self-expression and the communication of material intended to benefit the collective public (such as search engine indexing in example six)) and, secondly, the particularly careful balancing of rights and interests which is called for here.

Finally, whatever the nature of the new text, it is critical to recognize that the evidence above indicates that the current and, it would appear, the likely future stance of the DPAs is only partially related to the nature of the formal law. Instead, notwithstanding its clear tension with the open data paradigm which has become ubiquitous online, DPAs have been as influenced by an expansive cultural conception of the role of general data protection norms in society. Given this, it is imperative that any legislative change be combined with a broader engagement with DPAs as regards the need for a new reconciliation of rights within this area. This engagement should be coupled with a wider societal debate involving not just DPAs and the major new media actors but citizens generally. This process should lead to a recognition that, whilst many new media activities can pose a significant threat to data subject's rights and freedoms and are therefore rightly within the purview of data protection, explicit exemption from many of this law's detailed requirements are, in many cases, necessary in the interests of freedom of expression. If at least the essential elements of this understanding can be developed on a pan-European basis, then both a better balancing of rights on the internet and a reduction in the wide diversity of national approaches should result. Both the integrity and the legitimacy of European data protection would thereby be strengthened.

Conclusions

Notwithstanding its easily dismissed and often narrow conceptualization within public debate, the broad scope and purposes of the European data protection regime actually mandates a strong interaction and limitation of public freedom of expression. Moreover, as this article has demonstrated through the analysis of a wide-ranging survey answered by over 80% of national EEA DPAs together with six sub-national bodies, these important regulatory agencies have generally developed an expansive outlook as regards the extent to which default data protection norms are engaged vis-à-vis public expression on the 'new media'. Firstly, as regards the special purposes provision (Art. 9 of Directive 95/46) which was expressly designed to reconcile data protection with freedom of expression, a majority of DPAs have developed an understanding of its scope which, notwithstanding contrary CJEU pronouncements in *Satamedia*, gives priority to the institutional media and thereby removes many amateur bloggers from the protection of this shield. Secondly, although a significant number of DPAs at least partially adopted the rationale of *Lindqvist* by holding that, as regards rating websites and individual activities linked to self-expression such as social networking, general data protection provisions apply but must be interpreted with regard for freedom of expression (and related rights), a large number of others considered that no special interpretation was necessary even in these contexts. Finally, as regards the activity of the social networking sites themselves, street mapping services and search engines, the great majority of DPAs held that general data protection provisions must apply in full. Although aspects of the DPAs' expansive approach appear consonant with CJEU jurisprudence as most recently expounded in *Google Spain*,

the latter has itself been cogently criticised for failing to give appropriate weight to freedom of expression. Additionally to these overall patterns, the survey results also disclosed significant discrepancies in the interpretative stances between the DPAs. In particular, it is striking that, as regards all but two of the wide-ranging ‘new media’ examples presented, at least one DPA held that general data protection was applicable in full, whilst at least one other thought that data protection was entirely inapplicable. There is no direct relationship between these discrepancies and divergences in the national transposition of Directive 95/46. Nevertheless, a less regulatory interpretative stance on the part of DPAs as regards the ‘new media’ was associated with both a narrower *scope* and a greater *depth* of the special purposes derogation in national law.

Since 2012, Europe has been discussing proposals to reform data protection through the replacement of Directive 95/46 with a new Regulation. In this context, both the Council of the EU and the European Parliament have forwarded rewordings of the draft Regulation aimed at effecting a better balancing between data protection and freedom of expression. In particular, notwithstanding a number of continuing drafting difficulties, the Council of the EU text draws a helpful distinction between the special purposes and other forms of expression which are deserving of particular, but nevertheless more tightly circumscribed, shielding. Although reform of legislation in this area is clearly very important, this article has nevertheless demonstrated that DPAs’ interpretative stances are shaped at least as much by an expansive cultural conception of the role of data protection norms in society, as they are by the nature of formal legal provisions. Given this, any legislative change in this area must be accompanied by a broader debate and engagement with DPAs and society generally, both as regards ensuring minimum adherence to data protection standards in the new media sphere and, as importantly, the need for many such activities to benefit from explicit exemption from many of this law’s detailed requirements in the interests of freedom of expression. The successful crafting of such a new understanding would lead to a better protection of fundamental freedoms and also reduce the wide diversity of current national approaches. In contrast, in the absence of such engagement, the EU’s data protection regime will continue to fail to achieve true harmonisation and will also fuel increasing legal uncertainty as regards the enjoyment of human rights online.

Appendix: Quantitative Data from DPA Survey and Formal National Data Protection Law
N.B. Values in brackets represent imputed values (in italics if imputed from free-text response)

Data Protection Authority	Scope of Special Purposes Within Domestic DP Law	Continued Formal Applicability of DP to Special Purposes in Domestic DP Law (Erds (2015))	(0) Media Story	(1) Media Archive	(2) Amateur Blogger	(3) Rating Website	(4) Social Networker	(5) Social Networking Site	(6) Search Engine	(7) Street Mapping	(1)-(7) Generic DP Engagement Score
Austria	0.25 / (ii)	0.10	0.33/b	<i>(0.33/b)</i>	<i>(0.67/c)</i>	1/d	1/d	1/d	1/d	1/d	0.86
Belgium	0.75 / (iv)	0.61	0.33/b	0.67/c	0.33/b	1/d	1/d	1/d	0.67/c	1/d	0.81
Bulgaria	0.75 / (iv)	0.70	0.33/b	0.33/b	0/a	1/d	0/a	1/d	1/d	1/d	0.62
Croatia	0 / (i)	1.00	-	-	-	-	-	-	-	-	-
Cyprus	0.5 / (iii)	0.65	1/d	1/d	1/d	1/d	1/d	1/d	0.67/c	1/d	0.95
Czech Republic	0 / (i)	1.00	0.67/c	0.67/c	0.67/c	1/d	1/d	1/d	(1/d)	1/d	0.90
Denmark	1 / (v)	0.15	-	-	-	-	-	-	-	-	-
Estonia	0.25 / (ii)	0.67	0.33/b	0.33/b	0.33/b	1/d	1/d	1/d	1/d	1/d	0.81
Finland	0.75 / (iv)	0.00	0.33/b	0/a	0.33/b	0.67/c	<i>(0/a)</i>	1/d	1/d	1/d	0.57
France	0.75 / (iv)	0.53	0.33/b	0.33/b	0.67/c	1/d	1/d	1/d	1/d	1/d	0.86
Germany- Federal	0.25 / (ii)	0.03	0.33/b	0.33/b	0.67/c	0.67/c	0.67/c	0.67/c	1/d	1/d	0.71
Germany - Brandenburg	0.25 / (ii)	0.03	0.33/b	0.33/b	0.33/b	0.67/c	0.33/b	0.33/b	1/d	1/d	0.57
Germany – Mecklenburg-Vorpommern	0.25 / (ii)	0.03	0.33/b	0.33/b	0.67/c	0/a	1/d	1/d	1/d	1/d	0.71
Germany – Rhineland-Palatinate	0.25 / (ii)	0.03	<i>(0/a)</i>	<i>(0/a)</i>	<i>(0.33/b)</i>	0.67/c	0.67/c	<i>(0.67/c)</i>	1/d	1/d	0.62
Germany – Schleswig-Holstein	0.25 / (ii)	0.03	0.67/c	0.33/b	0.67/c	0.67/c	1/d	1/d	1/d	1/d	0.81
Gibraltar	0.75 / (iv)	0.33	0.33/b	1/d	0/a	1/d	0/a	1/d	1/d	1/d	0.71

Greece	0.5 / (iii)	0.84	0.67/c	0.67/c	0.67/c	0.67/c	0.67/c	0.67/c	1/d	1/d	0.76
Hungary	0.25 / (ii)	0.93	0.33/b	0.33/b	0.67/c	0.67/c	1/d	1/d	1/d	1/d	0.81
Iceland	1 / (v)	0.06	-	-	-	-	-	-	-	-	-
Ireland	0.75 / (iv)	0.34	0.67/c	0/a	0.67/c	0.67/c	0.67/c	0.67/c	0/a	0.67/c	0.48
Italy	0.5 / (iii)	0.65	0.33/b	0.67/c	0.33/b	0.67/c	0.67/c	0.67/c	1/d	1/d	0.71
Latvia	0.75 / (iv)	0.67	0.33/b	0.33/b	0.67/c	0.67/c	1/d	0.67/c	0.67/c	0.67/c	0.67
Liechtenstein	0.25 / (ii)	0.88	0.67/c	0.67/c	0.67/c	0.67/c	0.67/c	(0/a)	1/d	1/d	0.67
Lithuania	0.75 / (iv)	0.63	0.33/b	0.67/c	0.67/c	0.67/c	0.67/c	0.67/c	1/d	1/d	0.76
Luxembourg	0.75 / (iv)	0.68	0.33/b	0.67/c	0.67/c	1/d	1/d	1/d	1/d	1/d	0.90
Malta	1 / (v)	0.33	0.33/b	0.33/b	0.33/b	1/d	0/a	1/d	1/d	1/d	0.67
Netherlands	0.75 / (iv)	0.38	-	-	-	1/d	-	-	-	1/d	-
Norway	0.75 / (iv)	0.00	-	-	-	-	-	-	-	-	-
Poland	0.75 / (iv)	0.33	0.33/b	0.33/b	0.67/c	0.67/c	(0/a)	1/d	(1/d)	1/d	0.67
Portugal	0.75 / (iv)	0.77	0.67/c	(0.67/c)	0.67/c	0.67/c	1/d	1/d	1/d	1/d	0.86
Romania	0.75 / (iv)	0.83	-	-	-	-	-	-	-	-	-
Slovakia	0.75 / (iv)	0.93	0.33/b	0.33/b	0/a	1/d	(0/a)	1/d	0/a	1/d	0.48
Slovenia	0.25 / (ii)	0.93	(0.5)	(0.5)	(0.5)	1/d	0/a	1/d	1/d	1/d	0.71
Spain - Federal	0 / (i)	1.00	-	-	-	-	-	-	-	-	-
Spain - Catalonia	0 / (i)	1.00	0.67/c	0.67/c	0.67/c	0.67/c	0.67/c	1/d	1/d	1/d	0.81
Sweden	1 / (v)	0.00	0/a	0/a	(0.33/b)	1/d	(0.67/c)	(0.67/c)	(0/a)	(0.67/c)	0.48
UK	0.75 / (iv)	0.35	(0.33/b)	-	-	-	-	-	-	-	-