International Journal of Law and Information Technology, 2018, 26, 189–225
doi: 10.1093/ijlit/eay007
Advance Access Publication Date: 5 June 2018
Article

OXFORD

Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU *acquis*

David Erdos*

ABSTRACT

With the explosion of computer technology, vastly more and more varied types of data related to individuals are being disseminated online, often without their consent. While intermediary publishers are not the initial and immediate cause of this, they generally play a contributory role and engage in further (semi-)autonomous processing such as organizing or promoting content. Current case law rather haphazardly recognizes intermediary publishers to be data protection 'controllers' and/or protected by the intermediary 'host' shield, while also acknowledging the engagement of general human rights law. Seeking to synthetically balance the competing purposes which underlie these three legal frameworks, this article argues that greater responsibility should flow from more autonomous control but that some shielding is still necessary for all intermediary publishers. Conceptually it is argued that such a synthetic approach leads to intermediary publishers being grouped into three increasingly autonomous categories—'processor hosts', 'controller hosts' and 'independent intermediaries'—which should be subject to a successively greater ambit of responsibility accordingly. Detailed elaboration of the resulting duties must also take account of the seriousness of the potential interference with competing rights and, in this regard, should give weight to the divergent resource capacity of otherwise similarly situated actors.

KEYWORDS: Directive 2000/31, data protection, intermediary liability, privacy, Regulation 2016/679, reputation, right to be forgotten, social media

*University Senior Lecturer in Law and the Open Society, Faculty of Law and WYNG Fellow in Law, Trinity Hall, University of Cambridge. E-mail: doe20@cam.ac.uk. I would like to thank the many individuals who have made this research possible including, in particular, Krzysztof Garstka for his general assistance, Jef Ausloos, Frederik Borgesius and Bert-Jaap Koops for providing substantive feedback on a previous version of this manuscript and Niko Härting, Alessandro Mantelero and Marta Staccioli for help in the location of relevant materials. Some of research presented in this work was supported by the Economic and Social Research Council (ES/M010236/1) and also by a University of Cambridge CRASSH Early Career Fellowship. Any errors and all views expressed remain mine alone.

INTRODUCTION

The dramatic shift of our lives online has presaged revolutionary changes in the scale and nature of the (indeterminate) publication of all sorts of information or data including that related to identified or identifiable natural persons (hereinafter 'personal data'). Vastly more and more varied types of personal data are being published than ever before and such information is often subject to related but additional processing that promotes, aggregates, organizes and enables the ready retrieval of such content. The human rights impact of these developments have been ambiguous. While the enjoyment of freedom of expression[1] (as well as associated rights such as freedom to conduct a business)[2] has been hugely enhanced, individual protective rights over personal data[3] including the right to respect for private life and reputation[4] have generally suffered.

These radical developments have resulted from two very different types of actor, labelled hereinafter as original publishers and intermediary publishers. 'Original publishers' refer to those who issue the immanent instructions that result in a dissemination of personal data online. Although these actors are sometimes substantial organizations, they now primarily comprise hundreds of millions of natural persons who act in a non-professional capacity. These original publishers often publish personal data relating not only to themselves but also to third-party natural persons and it is with this latter category that this article concerns itself. Meanwhile, 'intermediary publishers' refer to actors who carry out publication activities directly linked to these acts of initial publication. As will be seen, this category is conceptually broad, ranging from those who perform limited acts explicitly under the instruction of original publishers to others who engage in far-reaching and essentially autonomous processing. Meanwhile, turning to questions of scale, although some intermediary publishers are small-scale, the majority of such processing is performed by substantial and sometimes enormous organizations.

Within the EU, data protection law, which has been principally specified in Data Protection Directive 95/46[5] but which from 25 May 2018 is replaced by General Data Protection Regulation 2016/679,[6] constitutes the primary framework regulating personal data processing. Although acutely conscious of the need for a 'free flow' of data at least within the EU itself[7] it is (as its name suggests) essentially concerned with protecting such data and in consequence the rights of individuals related to this such as the right to privacy.[8] Given this, at least when processing relates to publication activity, its default provisions often conflict with the right to freedom of expression. Such conflicts arise not only from the substantive standards it sets down but,

1 ECHR, art 10; EU Charter, art 11.
2 EU Charter, art 16.
3 EU Charter, art 8.
4 ECHR, art 8; EU Charter, art 7. See also ICCPR, art 17.
5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
7 Directive 95/46, art 1(2); cf Regulation 2016/679, art 1(3).
8 Directive 95/46, art 1(1); cf Regulation 2016/679, art 1(2).

in addition, from its default 'ambit of responsibility' which, by mandating that 'controllers' ensure comprehensive *ex ante* and *ex post* discipline over data processing, can pose particularly serious problems for intermediary publishers. This article concerns itself exclusively with the latter dimension, first through an essentially descriptive analysis of not only legislation but also Union and national-level case law and then through forwarding a new synthetic normative approach as to how the law should be interpreted and applied going forward.

Turning first to the descriptive analysis, reflecting European data protection law's broad protective purpose, most intermediary publishers have been classed by courts as data 'controllers'. Moreover, while this law does contains important derogatory provisions, these have only been explicitly deployed in relation to the substantive as opposed to ambit of responsibility dimension of this problem. Instead, attention has focused on the e-Commerce Directive 2000/31[9] which sets out a qualified responsibility shield for 'hosts' (and also for other, more limited intermediaries). Reflecting a broad interpretative approach, case law has found that this shield extends to a wide variety of intermediary publishers including blog platforms and social networking sites. A minority of Member States have also legislated for a generally cognate shield covering information location tools such as search engines. A substantial but loosely conceptualized overlap has therefore emerged between being a 'controller' and being a 'host' (or equivalent); nevertheless, some courts have interpreted a special clause in Directive 2000/31[10] as entirely excluding data protection matters from all these shields. Finally, a general human rights analysis has often been overlaid as an additional element, even when considering actors which may fall outside the 'host' shield.

Although ensuring greater coherence, certainty and balance in the law would be best achieved through comprehensive legal reform, Regulation 2016/679 only provides a gloss on the erstwhile *status quo*. In lieu, this article sets out a new synthesis of these three legal frameworks which develops along three dimensions. First, drawing on the competing ends which these frameworks pursue, three interlinked principles of interpretation are developed, namely, (i) that as an intermediary publisher exercises greater autonomous control over processing so the basis for it being subject to the various duties set out in codified data protection grows stronger and the legitimacy of deploying codified intermediary shields to prevent or severely limit this becomes weaker (ii) that, nevertheless, even when the codified intermediary shields are entirely inapplicable, certain shields may be required to protect freedom of expression (and related rights) and (iii) that in the elaboration of duties and also to preserve a rights balance, some account must be taken of the divergent 'capacities' of even similarly situated intermediary publishers given potentially vast divergences in their resourcing. Secondly, and at a conceptual level, the core definitions found within both codified data protection and intermediary shield law are mined to ensure that they all perform relevant work and none are over-stretched so as to unduly colonize this space. It is argued on this basis that intermediary publishers group into

9 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 (Directive on electronic commerce), in the Internal Market.

10 Directive 2000/31, art 1(5)(b).

three categories, namely, (i) those that are not only intermediary 'hosts' but also only data protection 'processors' (labelled 'processor hosts'), (ii) those which are intermediary 'hosts' but also data protection 'controllers' (labelled 'controller hosts') and (iii) those which are data protection 'controllers' and not intermediary 'hosts' (labelled 'independent intermediaries'). Finally, by integrating these two primary dimensions, an attempt is made to specify what the ambit of responsibility of each of these types of actors should be in the new era of Regulation 2016/679.

Following some definitional and historical background in the next section, the article descriptively explores current legislation and case law, looking first at the formal applicability of codified intermediary shield and data protection law and then at the specification of intermediary publisher responsibility under both of these frameworks. The 'Towards a New Synthetic Approach' section then turns to a normative synthetic analysis. Finally, the last section sets out some overarching conclusions.

DEFINITIONAL AND HISTORICAL BACKGROUND

Although terms such as 'intermediary' and 'publication' are widely used in the literature, the definition of both and especially the former are often left rather opaque. For the purposes of this article, 'intermediary publisher' refers to any online actor which is not immediately responsible for an initial publication of data but which performs publication-related processing directly linked to this initial act performed by the 'original publisher'. In carrying out such processing, these 'intermediary publishers' place themselves in some sense in an 'intermediate' position between the 'original publisher' and the end users of the information. The end users in this case are of an indeterminate nature since 'publication' is defined here in its strict sense of making or remaking information 'public' or, in other words, making it available to an indefinite number of persons. In this way, the qualification of the intermediary as a 'publisher' distinguishes these actors from those who merely transmit or communicate information to a predefined and limited number of persons.[11] Very often this published data relates not (or not only) to the original publisher themselves but rather to another identified or identifiable third-party natural person.

While all intermediary publishers share the commonalities just outlined, these actors differ profoundly as to what extent and how autonomously they perform 'value-added operations'[12] linked to third-party personal data. The most limited and least autonomous type of intermediary publisher provides 'simple' hosting by merely provisioning 'a server on which the provider rents space to users [the 'original publishers'] for content such as a web page, which may incorporate many kinds of information (software, texts, graphics, sound)'.[13] These services may additionally provide for the 'integration of tools' facilitating original publishers' creation and organization

11 Such a distinction is recognized in the definition of 'communication' (as opposed to 'publication') set out in the e-Privacy Directive. See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), art 2(d).

12 J Van Hoboken, 'The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember' (2013), 28. <http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf> accessed 27 April 2018.

13 R Julia-Barcelo, 'On-line Intermediary Liability Issues' (2000) 22 EIPR 106, 109.

of their content such as 'page templates' and 'ways to organize the information and link it'.[14] However, beyond this, intermediary publishers may themselves engage in a wide variety semi- or fully autonomous activities linked to this information (either *ab initio* or subsequent to first publication) including organizing, combining, aligning and/or retrieving the content.[15]

Intermediary publishers have been integral to public online systems right from their genesis in the 1970s and 1980s. Initially, 'simple' hosting services, sometimes with additional tool integration, dominated the scene.[16] The development of the World Wide Web in the 1990s and mobile apps in the 2000s and 2010s not only saw 'online' emerge into a truly mass phenomenon but also presaged the development of new types of powerful and significantly autonomous intermediary publisher, starting with generalized search engines and moving on to the array of profiling, sharing and most particularly social networking services now ubiquitous in today's 'Web 2.0'. Many of these services have tremendous reach and are underpinned by phenomenal resources.[17] Thus, the issues with which this article grapples involve a complex and variegated ecosystem that has come to penetrate 'every fiber of culture today'.[18]

CURRENT APPROACHES TO THE APPLICABILITY AND SPECIFICATION OF THE RESPONSIBILITY OF INTERMEDIARY PUBLISHERS UNDER CODIFIED DATA PROTECTION AND INTERMEDIARY SHIELD FRAMEWORKS

To ground the analysis, it is important to descriptively explore the applicability of the two key statutory frameworks in this area (namely, codified data protection and the codified intermediary shields) and, following on from this, also the specification of intermediary publisher responsibility under each of these. This section does so through an analysis not only of the formal legal provisions found in each codified framework but also case law at both Union level and in seven out of the eight most populous EU Member States.[19]

Applicability of European data protection to intermediary publishers

The legislative scheme

European data protection first emerged in the 1970s as an interventionist response to the perceived threat (now significantly realized) that computerization (including

14 M Cunha, L Marin and G Sartor, 'Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web' (2012) 2 IDPL 50, 51.

15 Such additional processing is often based on a monitoring of the preferences of the end users of these information services. However, the specific data protection issues which arise from such profiling lie beyond the scope of this article.

16 P Yates-Mercer, *Private Viewdata in the UK* (Gower 1985) 68.

17 Thus, Google/Alphabet's reported turnover in 2016 was $26.06bn, while Facebook's was $27.64bn in the same year. Meanwhile, Facebook alone had a staggering 1.86bn monthly active users as of the end of 2016. See Alphabet, 'Facebook Announces Fourth Quarter and Fiscal Year 2016 Results' (2017) <https://abc.xyz/investor/news/earnings/2016/Q4_alphabet_earnings/> accessed 27 April 2018 and Music Ally, 'Financials Reveal Facebook was a $26bn business in 2016' (2017) <http://musically.com/2017/02/02/financials-reveal-facebook-was-a-28bn-business-in-2016/> accessed 27 April 2018.

18 J van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (OUP 2013) 4.

19 Namely, Germany, France, the UK, Italy, Spain, Poland and the Netherlands.

computerized networks) might pose to the privacy and related personal rights of natural persons. Building on the Council of Europe Data Protection Convention of 1981,[20] in 1995 the EU adopted Data Protection Directive 95/46 using its internal market *vires*. Data protection's status was enhanced not only by the EU Charter recognizing it as a fundamental right in 2000,[21] but then by the Treaty of Lisbon granting this right primary law status and its own *vires* in 2009.[22] The new General Data Protection Regulation 2016/679 was adopted under this new *vires* in 2016 as a key plank of the European Commission's Digital Single Market strategy. It applies from 25 May 2018.[23]

Reflecting its broad purposes, European data protection has from its inception been 'deliberately cast widely'.[24] Thus, by default, Directive 95/46 regulated all 'processing of personal data wholly or partly by automatic means'[25] carried out by or under the authority of data 'controllers'. It defined all these terms broadly. '[C]ontroller' referred to anybody which 'alone *or jointly* with others determines the purposes and means of the processing of personal data',[26] 'personal data' was defined as '*any information* relating to an identified or identifiable natural person ('data subject')'[27] and 'processing . . . by automatic means' covered '*any operation*'[28] performed digitally including storage, dissemination and organization. Two narrow exceptions qualified this material default – one for processing 'by a natural person in the course of purely personal or household activity' and another for activity 'outside the scope of Community law'[29]—but neither had application to private sector organizational activity.[30] Finally, the Directive specified the concept of 'processor'—defined as anybody who processes personal data 'on behalf of a controller'[31]—detailing that these actors had to be controlled indirectly by the relevant controller *inter alia* ensuring through a written binding legal act that they 'act only on instruction'.[32]

20 Directive 95/46, recital 11.
21 EU Charter, art 8.
22 TFEU, art 16.
23 Regulation 2016/679, art 99(2).
24 United Kingdom, Lindop Committee on Data Protection, *Report* (HMSO 1978) 147.
25 Directive 95/46, art 3. As this article also specified, processing personal data linked to a structured manual filing system was also covered.
26 Directive 95/46, art 2(d) (emphasis added); cf Regulation 2016/679, art 4(7).
27 Directive 95/46, art 2(a) (emphasis added); cf Regulation 2016/679, art 4(1).
28 Directive 95/46, art 2(b) (emphasis added); cf Regulation 2016/679, art 4(2).
29 Directive 95/46, art 3(2); cf Regulation 2016/679, art 2(2).
30 Thus, the first not only expressly covers the 'processing of data carried out by the natural person [rather than an organization]' but moreover the phrase 'purely personal or household' was interpreted in *Criminal proceedings against Bodil Lindqvist* (C-101/01) EU:C:2003:596 as relating only to 'activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people' (at [47]). Meanwhile the second simply mirrored the Directive's internal market *vires* and was confirmed in *Lindqvist* to relate only to 'the activity of State or State authorities' (at [42]).
31 Directive 95/46, art 2(e); cf Regulation 2016/679, art 4(8).
32 Directive 95/46, art 17(3); cf Regulation 2016/679, art 28(3).

The Directive did not grant Member States any discretion as regards its material scope and essential definitions[33] and, in general, these provisions were faithfully transposed.[34] Meanwhile, Regulation 2016/679 generally mirrors these provisions. It further stresses that, irrespective of the applicability of the 'personal or household' exemption to natural persons, its provisions 'should apply to controllers or processors which provide the means for such personal or household activities'.[35]

Relevant CJEU and national case law

Although the earliest regulatory attempts to apply European data protection to intermediary publisher activity date to the mid-1980s,[36] relevant case law is confined to the Directive 95/46 era. Reflecting the broad material scope of codified European data protection, both national courts and the CJEU have found a wide variety of intermediary publishers to be 'controllers'. Thus, although Spanish courts have recently found that this was at least not proved in relation to the blog hosting service Google Blogger,[37] such status has been ascribed to the following operators:

- a blogging service shown to organize posts anti-chronologically over time and with terms allowing it to suspend transmission in case of abuse,[38]
- evaluation sites concerning teachers,[39] doctors[40] and law professionals,[41]
- a profiling site for grandparents estranged from their grandchildren enabling a telling of their story and allegedly aimed at a renewal of contact,[42]
- internet search engines,[43]

33 While Directive 95/46 sets out a number of sometimes wide-ranging derogatory provisions (notably in arts 9 and 13) none provided any exception from its general provisions as regards object, definitions, scope or national law applicable (arts 1–4).

34 Certain problems were identified in a few Member States but even these would appear minor in this context. For a discussion of the UK case see R Jay, *Data Protection Law and Practice* (4th edn, Sweet & Maxwell 2012) 18–20.

35 Regulation 2016/679, recital 18.

36 As early as 1983 the International Conference of Data Protection Commissioners expressed general concern about this area ('Data Protection in the New Media' (1984) 8 TDR 416). Meanwhile, in the mid-1980s the French DPA argued that those running romance sites on the online Minitel system could be held criminally responsible under national data protection law in certain circumstances as a result of being a party to their users maliciously and anonymously publishing the name and telephone number of other natural persons on the site (see France, Commission national de l'informatique et des libertés, *7e rapport d'activité 1er janvier 1986 – 31 décembre 1986* (Documentation Française, 1987) 155–56). Although it is beyond the scope of this article to further consider this, it is clear that the degree of responsibility the French DPA expected of these services was very considerable.

37 See Audencia Nacional, 29 December 2014, ECLI:ES:AN:2014:5252; Audencia Nacional, 29 December 2014, ECLI:ES:AN:2014:5254; Audencia Nacional, 17 February 2015, ECLI:ES:AN:2015:661 and Audencia Nacional, 24 February 2015, ECLI:ES:AN:2015:568.

38 See *Mr X v Overblog* (Cour d'appel de Montpellier, 22 March 2017).

39 See *Note2be.com Ltd, Mr SC v La Federation Syndicale Unitaire and Ors,* 08/04727 (Cour d'appel de Paris, 25 June 2008) and *Spichmich de*, VI ZR 196/08 (Bundesgerichtshof, 2009).

40 Polish Supreme Administrative Court, 21 April 2015 (I OSK 1480/14).

41 *Law Society, Hine Solicitors and Kevin McGrath v Rick Kordowski* [2011] EWHC 3185 concerning the evaluation/shame site Solicitors from Hell.

42 Rechtbank Utrecht, 276 630/KG ZA 09-5161, ECLI:NL:RBUTR:2009:BJ1409.

43 Determined not only at pan-EU level in *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González v AEPD* (C-131/12) EU:C:2014:317 [2014] but prior to

- social networking sites[44] and
- a video-sharing service.[45]

In the main, the findings here have been quite general. In contrast, at least in the *Google Spain*[46] and Google Video[47] cases, which concerned search engines and video-sharing services respectively, they targeted particular publication-related processing operations. However, since this targeting appears to have resulted from an attempt to proportionately reconcile data protection with intermediary shield law and/or other fundamental rights, this aspect relates more to the specification of responsibility rather than the applicability of the law *per se*. As a result, discussion on this point will resumed in the 'Specification of responsibility under European data protection' subsection below.

Applicability of European intermediary shield law to intermediary publishers

The legislative scheme

In contrast to European data protection's interventionist origins dating back to the 1970s, European intermediary shield law emerged only in the late 1990s as part of a principally economic[48] but also freedom of expression-related[49] initiative to liberalize markets for the 'information society services'[50] which were rapidly developing. In significant contrast to the scheme implemented in the USA[51] and favoured by some civil society groups,[52] the resulting shields are narrowly focused on three discrete intermediary activities. First, 'mere conduit' activity defined as 'the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network'.[53] Secondly, performing 'caching'

this in *Mme C v Google France and Google Inc* (Tribunal de Grande Instance de Monpellier, 28 October 2011) as regards Google's core search services and *Diana Z v Google* (Tribunal de Grande Instance de Paris, 15 February 2012) as regards its autosuggest functionality.

44 Determined in Polish Supreme Administrative Court, 18 November 2009 (I OSK 667/09) as regards Nasza Klasa and *CG v Facebook Ireland Ltd, Joseph McCloskey* [2016] NICA 54 as regards Facebook.

45 *Milan Public Prosecutor's Office v Drummond et al* (5107/14) (2013) (Corte di Cassazione) as regards Google Video.

46 See n 43.

47 See n 45.

48 See art 1 as well as recitals 2, 5, 6, 7, 21, 40 and 60 of Directive 2000/31.

49 See recitals 9 and 46 of Directive 2000/31.

50 Such services were defined as those 'normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, at the individual request of a recipient of a service', with remuneration construed broadly such that 'in so far as they represent an economic activity, [this] extend[s] to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data'. See Directive 2000/31/EC, Recitals 17 and 18.

51 Thus, subject to exclusions in the areas of federal criminal law enforcement and intellectual property, s 230(c)(1) of the US Communication Decency Act 1996 simply protects any and all 'interactive computer service[s]'. Meanwhile, the Digital Millennium Copyright Act (DCMA) 2000 does establish a more targeted regime in the area of copyright, but nevertheless provides explicit protection for 'information location tools' (s 512(d)), a provision which is not reflected in the pan-EU scheme at all.

52 Thus, the Manila Principles on Intermediary Liability (2015) <https://www.manilaprinciples.org/> accessed 27 April 2018 speaks broadly of protecting actors which facilitate communication over the internet, although the examples its gives here are confined to internet access providers, social networks and search engines.

53 Directive 2000/31, art 12(1).

in the context of conduit activity, defined as 'the automatic, intermediate and temporary storage of [the] information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request'.[54] Finally, and most relevantly, 'hosting' defined as 'the storage of information provided by a recipient of the service' at their 'request' and where the recipient is not 'acting under the authority or the control of the provider'.[55] The initial examples[56] given of services covered by this latter shield were limited to 'simple' hosting.[57] However, following the concerns of Germany and Greece, the Commission agree to a reformulation 'to clarify that it covered active as well as passive hosting'.[58] Ultimately, however, no rewording eventuated. Finally, it was also decided not to shield 'location tool services' but rather only to re-examine this issue later.[59]

Alongside these general provisions, the Directive included a specific data protection clause stating that it did not apply to 'questions relating to information society services' covered by Directive 95/46.[60] As originally drafted, this clause referred rather to 'the field covered by' this Directive,[61] a phrasing which was clearly aimed at completely excluding data protection from the general e-Commerce framework[62] (justified on the basis that EU data protection dealt with the 'liability' not of intermediaries but of controllers[63] and already provided for free movement within the internal market[64]). Although a few Member States questioned this approach,[65] even after rephrasing the clause was still described as providing an 'exemption' for 'data

54 Directive 2000/31, art 13(1). In this regard, the Commission stressed from the outset that such 'system caching' was confined to storage undertaken 'with a view to enhance the performance and speed of digital networks' and 'does not constitute as such a separate exploitation of the information transmitted'. See European Commission *Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market Explanatory Memorandum* (COM (1998) 586 Final) 28–29.

55 Directive 2000/31, art 14 (1)-(2).

56 Namely the 'provision of server space for a company's or an individual's web site, for a BBS [Bulletin Board Service], a newsgroup, etc.' (European Commission (COM (1998) 586 final) 29).

57 See similar analysis in C Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer 2013) 81.

58 Council Document 8891/99 (3 June 1999).

59 Directive 2000/31, art 21(2). The idea of such a liability shield was raised by Ireland during the Council's deliberations on the Directive but did not secure the support of any other Member State. See European Union, Council Document 12957/999 EXT 1 (23 November 1999) 4.

60 Directive 2000/31, art 1(5)(b). A more specialized telecommunications instrument (Directive 97/66/EC) was similarly reference. This directive has now been replaced by Directive 2002/58 and so this reference now refers to the latter instrument.

61 See art 22(1)(b) of COM (1998) 586 final ('the field covered by Directive 95/46/EC') and art 22(1)(b) of COM (1999) 427 final ('the field covered by Directives 95/46/EC and 97/66/EC').

62 See, for example, Council Document 7085/99 (31 March 1999).

63 See Council Document 6144/99 (Annex Working Party—Table on Relationship with Other Community Directives) (23 February 1999) 10 stating that '[t]he e-commerce proposal does not affect directives which deal with liability in respect of other activities i.e. which do not address the specific activity of intermediaries. Examples . . . "Data protection" Directive 95/46/CE [sic] and Directive on personal data and privacy in the telecommunications sector 97/66/EC: Both deal with the liability of the controller of the personal data'.

64 See Council Document 6144/99 at 7 stating that the e-Commerce Directive's internal market clause was 'coherent with other directives and proposals concerning electronic media, for example . . . "Data protection" Directive 95/46/EC'.

65 See Council Document 70085/99 (31 March 1999) detailing comments made by the Netherlands, Portuguese and UK delegations.

protection aspects',[66] an understanding reinforced by an accompanying Recital which remained based on the initial wording.[67] Under Regulation 2016/679, references to Directive 95/46 must be construed as references to this new Regulation.[68] Nevertheless, this new Regulation provides a liberalizing gloss on this clause's meaning by stating that its codification of data protection 'shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service provides in Articles 12 to 15 of that Directive'.[69]

Turning to Directive 2000/31s transposition, a clear majority of Member States have set out the scope of the liability shields 'almost verbatim' as in the Directive,[70] although some have not (at least explicitly) made provision for the data protection clause.[71] In addition, although not provided for in the Directive itself, a few Member States have also set out a shield for information location services such as search engines.[72]

Relevant CJEU and National Case Law

To date, the CJEU has interpreted the intermediary shields as regards an intermediary publisher's own processing only within the context of the enforcement of intellectual property as opposed to, say, data protection rights.[73] In doing so, it has exclusively focused on the 'hosting' shield, interpreting this provision very broadly. Thus, in *Google France v Vuitton* (2010), a Grand Chamber held that an advertising reference service could in principle be a 'host'[74] and in *L'Oréal v eBay* (2011) another Grand Chamber ruled likewise as regards an online marketplace. *L'Oréal* further explicitly suggested it was sufficient that a service merely '*includes* the storage of information transmitted to it by its customer-sellers'[75] rather than that it '*consists* of the storage of information provided by a recipient' as set out in the Directive itself.[76] Reflecting this, in *SABAM v Netlog* (2012) the CJEU proceeded on the basis that an 'online social networking platform' could be a 'host'.[77] Nevertheless, in both *Google*

66 See Council Document 12667/99 (15 November 1999) 3.

67 In sum this *inter alia* stated that '[t]he protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC . . . and Directive 97/66/EC . . . which are fully applicable to information society services' (Directive 2000/31/EC, Recital 14).

68 Regulation 2016/676, art 94.

69 ibid art 2(4) and also recital 21.

70 P Van Eecke and others, *Liability of Online Intermediaries* (2009) 19 <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=835> accessed 30 April 2018.

71 For one such example see Spain, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

72 See data set out at [89]–[105] in *Metropolitan International Schools Ltd (trading as Skillstrain and/or Train2Game) v Designtechnica Corpn (trading as Digital Trends) and others* [2009] EWHC 1765 (QB) detailing seven EU states which provide for such a shield in their national law, namely, Austria, Bulgaria, Hungary, Portugal, Romania and Spain.

73 On the other hand, in *Productores de Música de España (Promusicae) v Telefónica de España SAU* (C-275/06) EU:C:2008:54 [2008] the CJEU did consider in what circumstances intermediary publishers might have an obligation to accede to a request to provide details of their users in the context of civil proceedings to defend intellectual property rights notwithstanding its data protection obligations to those users.

74 *Google France and Google Inc v Louis Vuitton Malletier SA* (C-256/08) EU: C:2010:159 [2010] at [111].

75 *L'Oréal v eBay* (C-324/09) EU:C:2011:474; [2011], at [111] (emphasis added).

76 Directive 2000/31, art 14(1) (emphasis added).

77 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (C-360/10) EU:C:2012:86; [2012] at [27].

France and *L'Oréal* the Court stressed that any activity must remain within Directive 2000/31's concept of an 'intermediary' which it elaborated as one which was 'mere[ly] technical, automatic and passive pointing to a lack of knowledge or control of the data which it stores',[78] a definition further specified in *L'Oréal* as requiring that the provider adopt a 'neutral position'[79] between the original uploader and the end user. However, in further elucidation, the Court adopted a rather liberal approach to these limits finding that, while active assistance could vitiate the shield,[80] the exercise of generic control over a service would not do so.[81]

Turning to the national level, for reasons of both practicality and focus, consideration of jurisprudence on the interface between the shields and intermediary publishers will be confined to cases with data protection as a cause of action. In some of these cases, such causes of action have been excluded from the shields entirely, usually[82] but not invariably[83] through an explicit reference to the data protection clause. Meanwhile, in the merely interlocutory decision of *Mosley v Google* the England and Wales High Court left this issue open.[84] In contrast, however, in *CG v Facebook Ireland, McCloskey* (2016) the Northern Ireland Court of Appeal not only found Facebook to be a 'host'[85] but held that a damages claim against it for publishing in

78 *Google France* at [114] cited also in *L'Oréal* at [113]. Although this phrasing drew on recital 42 of Directive 2000/31 it appears that this recital was originally intended to relate only to the mere conduit and caching shields. Nevertheless, largely the same idea is found in art 14(3) on hosting which states this shield 'shall not apply when the recipient of the service is acting under the authority or the control of the provider'.

79 *L'Oréal* at [116].

80 Thus, in *L'Oréal* the Court held that activity would go beyond these limits where 'the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting these offers' (at [113]), while in *Google France* it found this could also result from 'the role played by Google in drafting of the commercial message which accompanies the advertising link or in the establishment or selection of keywords [in AdWords]' (*Google France* at [118]).

81 Thus, in *L'Oréal* it found that the shield could apply even if an 'online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers' (at [115]) and in *Google France* it ruled that this was similarly the case even if 'the resulting display of ads is made under conditions which Google controls' and that 'Google determines the order of the display according to, inter alia, the remuneration paid for by the advertisers' (at [115]).

82 Examples which reference this clause including the Netherland's grandparent estrangement site case (ECLI:NL:RBUTR:2009:BJ1409 at [5.8]) and Corte di Cassazione's *Google Video* judgment (*Milan Public Prosecutor's Office v Drummond et al* (5107/14) (2013)), although in the latter case a similar outcome was achieved through a narrowing of the material scope of data protection (see 'Specification of responsibility under European data protection' subsection).

83 For example, without mention of this clause, a 2015 Italian judgment concerning deindexing from Google search engine implied that Google's general obligation to manage its index in line with data protection was not covered by the shields; conversely it held that a reputation claim arising from allegedly false information found through a particular web link was limited by the 'caching' shields. See Tribunal Ordinario di Roma, 24 November 2015 (RG 79860/2014).

84 Apart from the applicability of the prohibition of general monitoring (Directive 2000/31, art 15) on which not even a provisional view was formed, the Court expressed a provisional preference for the view that data protection and intermediary shield law 'must be read in harmony and both, where possible, must be given full effect to' (*Mosley v Google Inc & Or* [2015] EWHC 59 (QB) at [43]). Moreover, assuming intermediary shield law did apply, it saw the Google image search engine falling within the provision on 'caching' (at [53]).

85 [2016] NICA 54 at [53] (wrongly citing this as art 15 rather than 14 of Directive 2000/31). Interestingly, despite defining the shield very narrowly as covering only services which offer 'only the

violation of data protection was not a 'question relating to information society services covered by the [. . .] Data Protection Directives'[86] and so the 'host' shield could continue to apply.[87] Other cases have explored the applicability of the intermediary shields without considering whether data protection should be differentiated from other legal actions. In *Spickmich* (2009), the Bundesgerichtshof stated that, by organizing ratings, this teaching evaluation website may have adopted the content, thus bringing its activity outside of the shields; ultimately, however, it found this did not need to be decided.[88] In contrast, in *Diana Z. v Google* (2012) the Tribunal de Grande Instance de Paris held that when indexing personal data the Google search engine was in principle protected by the 'host' shield.[89] Meanwhile, in a 2014 judgment the Heidelberg Landesgericht found that an internet search engine could not invoke either the 'mere conduit' or 'caching' shield since, by sorting and displaying the results in a specific order, Google was maintaining information for its own use. The potential for the service to invoke the 'host' shield was in principle left open.[90] On appeal, the Oberlandesgericht Karlsruhe did not explicitly address these issues.[91] Finally, in both France and Spain the 'host' shield has been applied to blogging services[92] and in Spain the national *sui generis* shield for information location tools has been applied to search engine services,[93] with at least one court explicitly stating that Directive 2000/31 itself provided no shield as regards the latter activity.[94]

Specification of responsibility under intermediary shield law

The legislative scheme

It is a cardinal principle that the e-commerce intermediary shields do not establish legal responsibility but only set out certain protections against those which otherwise would apply. However, in significant contrast to the shields implemented in the

storage of information provided by a recipient of the service', the Court nevertheless found that this 'clearly includes Facebook'.

86 *CG v Facebook Ireland, McCloskey* at [95].

87 On the other hand, in *NT1 NT2 v Google LLC* [2018] EWHC 799 (QB) Google sought to rely on the 'caching' shield vis-à-vis a data protection claim against its search service but, after the UK Information Commissioner's Office intervened to argue that the data protection clause entailed that such shields had no application here, it abandoned this (at [50]). See further V. Gladicheva, 'Google can't escape "right to be forgotten" damages, privacy regulator tells UK court' (2018) <https://mlexmarketinsight.com/insights-center/editors-picks/Data-Protection-Privacy-and-Security/europe/google-cant-escape-right-to-be-forgotten-damages,-privacy-regulator-tells-uk-court> accessed 27 April 2018.

88 Bundesgerichtshof, 23 June 2009, VI ZR 196/08.

89 *Diana Z. v Google*.

90 Landesgericht Heidelberg, 9 December 2014, 2 O 162/13. In another case, the Oberlandesgericht Köln, 13 October 2016, 15 U 173/15 found that a search engine should be covered by the intermediary shields and, most probably, by that of the caching or hosting provision. Ultimately, however, it found it unnecessary to finally determine this. An appeal upholding the outcome of this court did not address this specific issue. See Bundesgerichtshof, 27 February, VI ZR 489/16.

91 Oberlandesgericht Karlsruhe, 14 December 2016, 6 U 2/15. This case is now on a further appeal before the Bundesgerichtshof.

92 See *Mr X v Overblog*, Cour d'Appel de Montpellier, 22 March 2017 and Audiencia Nacional, 29 December 2014, ECLI:ES:AN:2014:5252.

93 See eg *Mr X v Overblog* and Audencia Nacional, 29 December 2014, ECLI:ES:An:2014:5129 (*Costeja* judgment).

94 Audencia Provincial de Barcelona, 17 July 2014, ECLI:ES:APB:2014:8246.

USA[95] and favoured by some civil society groups,[96] this protection is intended to differ profoundly depending on the type of activity pursued and (especially as regards 'hosting') is also intended to be significantly constrained. The conditional nature of immunity from civil and criminal liability for 'mere conduits' and 'caching' is principally[97] tied back to the limited definitional scope of these activities.[98] In contrast, the 'hosting' shield is specifically conditioned on the service acting 'expeditiously' to remove or disable access to material after obtaining 'actual knowledge' of its illegality or as regards claims for damages even 'aware[ness] of facts or circumstances' which make this 'apparent'.[99] According to recital 46, however, this is subject to observance of the principle of freedom of expression including any procedures in this regard laid down at national level; the permissibility of such procedures is also provided for in article 14(3) itself. Alongside these immunity provisions, article 15(1) prohibits Member States from imposing general monitoring obligations on these services,[100] although recital 47 stresses that this does 'not concern monitoring obligations in a specific case' and in particular does 'not affect orders by national authorities in accordance with national legislation'. Moreover, and also critically, recital 48 states as regards 'hosts' that Member States can still 'apply duties of care which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities'. Article 15(2) also specifically allows Member States to establish obligations on services to promptly inform competent authorities of alleged illegality or, in the case of hosts, even to provide on request information enabling the identification of those with whom they had storage agreements. Finally, the Directive explicitly states that both courts and administrative authorities retain, in accordance with Member States' legal systems, an injunctive ability to require that any service terminate or even prevent an infringement of law.[101]

95 Subject to exclusions in the areas of federal criminal law enforcement and intellectual property, s 230(c)(1) of the US Communication Decency Act 1996 not only protects all 'interactive computer service[s]' (see above note 51) but appears to grant these services complete immunity at least as regards expressive causes of action. In contrast, in the area of intellectual property only, the Digital Millennium Copyright Act (DMCA) 2000 sets out a scheme which is much more similar to that implemented in Europe.

96 For example, the *Manila Principles on Intermediary Liability* (2015) (above note 52) simply advocates that any and all 'intermediaries' should never be required to restrict content absent a specific order by a judicial authority and should never be required to monitor content proactively.

97 Even here, however, the Directive additionally mandates as regards 'caching' that the service expeditiously removes or disable access to information not only after obtaining 'actual knowledge' that information at the initial source had been disabled but even after becoming similarly knowledgeable that 'a court or an administrative authority has ordered such removal or disablement' (Directive 2000/31, art 13(1)(e)).

98 Thus, the 'mere conduit' shield stipulates that the service cannot initiate, select the receiver of or select or modify the information contained in any transmission (Directive 2000/31, art 12(2)), whereas the one for 'caching' provides that the service cannot modify the information and must comply with conditions on access to the information and with rules regarding its updating (Directive 2000/31, arts 13(1)(a)-(c)).

99 Directive 2000/31, art 14(1).

100 Defined as either 'a general obligation . . . to monitor the information they transmit or store' or 'a general obligation to seek facts or circumstances indicating illegal activity'.

101 Directive 2000/31, arts 12(3), 13(2) and 14(3).

In transposing these provisions, most Member States adopted the Directive's wording 'almost verbatim',[102] resulting in only rather subtle differences.[103] Nevertheless, as previously noted, a few also set out an explicit exemption for information location tool services such as search engines, usually modelled on the Directive's 'hosting' but sometimes on its 'mere conduit' provisions.[104]

Relevant CJEU and National Case Law

To date, CJEU case law in this area has not only been confined to intellectual property disputes but has also not yet provided anything like a comprehensive interpretation of all relevant provisions. *L'Oréal* deployed the concept of a 'diligent economic operator' here, finding that the 'awareness' threshold for damages would be exceeded if the service was 'aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality'[105] and then failed to act 'expeditiously' to address this thereafter;[106] the Court also stated that, while any notification given to the service must always be taken into account, the gaining of awareness by any means was sufficient including through 'an investigation undertaken on [the service's] own initiative'.[107] Turning to permissible injunctive relief, the Grand Chamber found that such a service could be mandated 'to take measures that contribute not only to bringing to an end infringements . . . but also to *preventing further infringements*'.[108] At the same time it held that, given article 15(1)'s prohibition on general monitoring, such duties 'cannot consist in an active monitoring of all the data of each of the customers in order to prevent any future infringement of intellectual property rights via that provider's website'.[109] Meanwhile, *SABAM v Netlog* found that an injunction requiring Netlog to indefinitely filter almost all the files placed on its service for potential violation of the IP rights SABAM claimed or would in the future claim constituted prohibited general monitoring.[110] The Court also found that this would fail to strike a 'fair balance' between the right to protection of intellectual property and the freedom to conduct a business, as well as potentially infringing user's right to the protection of personal data and their freedom to receive and impart information (an aspect of freedom of expression).[111]

102 See above note 70.

103 For example, in contrast to the Directive's 'hosting' shield (see above note 99) a number make no differentiation between 'actual knowledge' and 'awareness knowledge' (see reference at note 70). Meanwhile, some do not explicitly prohibit general monitoring. See eg UK, Electronic Commerce (EC Directive) Regulations 2002.

104 Thus, Spain, Portugal, Hungary and Romania all set out a provision here based on the 'hosting' shield, while Austria and Bulgaria provide for one based on that for 'mere conduits' (see above note 72).

105 *L'Oréal* at [120].

106 *L'Oréal* at [124].

107 *L'Oréal* at [122].

108 *L'Oréal* at [131] (emphasis added).

109 *L'Oréal* at [139]. General monitoring in this context was additionally found to violate the Intellectual Property Enforcement Directive 2004/48's requirement that measures here be fair, proportionate and not excessively costly.

110 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (C-360/10) EU:C:2012:86; [2012] at [38].

111 C-360/10 *SABAM v Netlog* at [47]–[48].

Turning to national case, a broad consensus has emerged that the intermediary shields do not protect intermediary publishers from having to comply with data subject's rights to erase illegal content[112] or even raise objection[113] to processing *ex post*. Thus, the *Diana Z v Google* (2012) case in France construed the 'host' shield such that Google still had to respond to the data subject's right to object and deindex specified links where warranted, while in *Mr X v Overblog* (2017) it ruled likewise as regards a blogging service.[114] The Spanish courts have similarly construed their *sui generis* shield for search engines[115] (which is modelled on the pan-EU one for 'hosting'[116]) such that these entities must still respond to such data subject requests, irrespective of whether the material linked to is itself lawful.[117] Meanwhile, the potential impact of the prohibition on general monitoring has been directly explored in a couple of UK interlocutory decisions. In both *Mosley v Google* (2015) and *AY v Facebook* (2016), the Court found that, even if this prohibition applied to data protection, the blocking of specified illegal sexual images on Google search[118] and sexualized images of the data subject as a child on Facebook[119] respectively might well not amount to general monitoring but only to a permissible specific blocking of content. On the other hand, the latter case found that blocking pages 'with the title "Shame Page" or with that title combined with another identifying issue' would be impermissible since '[t]he title "Shame Page" is consistent with both lawful and unlawful activity and to block all shame pages would be an interference with [European Convention] Article 10 rights of freedom of expression unless Facebook monitored the individual pages and such monitoring is impermissible'.[120] Finally, German courts have tended to adopt the position that injunctive relief remains in principle unaffected by the liability shields.[121] Nevertheless, in delineating permissible injunctions concerning personal data, German courts have often given emphasis to the need to proportionately balance competing fundamental rights. These important considerations will be addressed towards the end of the next subsection which turns to consider the specification of legal responsibility under data protection law.

112 Directive 95/46, art 12(b); cf Regulation 2016/679, art 17.

113 Directive 95/46, art 14; cf Regulation 2016/679, art 21.

114 *Mr X v Overblog*, Cour d'appel de Montpellier, 22 March 2017. In this case, the services' failure to accede to a *bona fide* right to object to the processing of personal data over an eighteen-month period resulted in the awarding of €7.5k non-pecuniary damages.

115 Spain, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, art 17.

116 See above note 104.

117 See for example, ECLI:ES:AN:2014:5129 (*Costeja* case). Google in this test case had *inter alia* argued that it only had to act if had acquired knowledge of the illegality of the underlying content.

118 *Mosley v Google* at [52].

119 *AY, a minor acting by FY as next friend v Facebook (Ireland) Limited & others* [2016] NIQB 76 at [12] stating that adoption of 'PhotoDNA [technology] in the context of sexualised images of a child may amount to [permissible] "blocking" as opposed to [impermissible] "monitoring"'.

120 *AY v Facebook* at [13].

121 See, for example, the Bundesgerichtshof, 23 June 2009, VI ZR 196/08 judgment (*Spickmich*) and the following Google deindexing judgments—Landgesgericht Hamburg, 7 November 2014, O 660/12, Landesgericht Heidelberg, 9 December 2014, 2 O 162/13, Oberlandesgericht Karlsruhe, 14 December 2016, 6 U 2/15. Note, however, that CJEU case law on this issue was mentioned in Oberlandesgericht Köln, 13 October 2016, 15 U 173/15 but not further addressed on appeal in Bundesgerichtshof, 27 February 2018, VI ZR 489/16.

Specification of responsibility under European data protection

European data protection's legislative scheme

By default, European data protection requires that controllers ensure that their processing comply with a broad set of data principles (together with a legal basis for processing),[122] rules ensuring that processing is transparent and that data subjects have rights to erase, rectify or block/restrict illegally processed data or sometimes even object to processing on personal grounds,[123] rules which generally ban the processing of sensitive data absent waiver from the data subject[124] and disciplining provisions aimed at ensuring that these provisions are not undermined by, for example, lax security.[125] Collectively, these obligations imply responsibility to ensure not only *ex post* but also *ex ante* discipline over processing. At the same time, Member States are obligated to adopt derogations for journalistic and cognate forms of 'special expression' if 'necessary to reconcile' the right to privacy or data protection with freedom of expression (including its subright, freedom of information).[126] Further clauses permit Member States to adopt other limited derogations where 'necessary' to safeguard 'the rights and freedoms of others'.[127] Under Directive 95/46, Member States' transposition of these derogatory provisions focused on qualifying the substantive obligations applicable to controllers engaged in certain types of expression, rather than in limiting the ambit of their responsibility.[128]

Regulation 2016/679 sets out strengthened default controller duties[129] and data subject rights.[130] In particular, it bolsters the right to erasure with a new 'right to be

122 Directive 95/46, arts 6–7; Regulation 2016/679, arts 5–6.

123 Directive 95/46, arts 10–12 and 14; Regulation 2016/679, arts 12–21.

124 Directive 95/46, art 8; Regulation 2016/679, arts 9 and 10. Directive 95/46 broadly and categorically defines sensitive data to include data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership', data 'concerning health or sex life' and data 'relating to offences, criminal convictions or security measures'. Regulation 2016/679 slightly rewords the protection of criminal-related data and also specifically protects 'genetic data', 'biometric data for the purpose of uniquely identifying a natural person' and 'data concerning . . . sexual orientation'.

125 Directive 95/46, arts 17–19, 21 and 25–46; Regulation 2016/679, arts 24–49.

126 Directive 95/46, art 9 (referring to 'privacy'); Regulation 2016/679, art 85(2) (referring to 'the right to the protection of personal data').

127 See Directive 95/46, art 13 and Regulation 2016/679, art 23. Both instruments contain certain cognate provisions, namely, Directive 95/46, arts 8(4), 8(5), 14(a) and Regulation 2016/679, arts 9(2)(g), 10. Collectively, these provisions allow for qualified derogations from the transparency provisions, control rights, sensitive data rules and, in relation to Directive 95/46 only, the data protection principles themselves.

128 In sum, under Directive 95/46, all but three Member States set out a substantive qualification for special expression, although its scope and especially depth exhibit marked divergences. Meanwhile, almost no Member State expressly deployed the other limited derogations to set out specific limitations beyond the area of special expression as they have defined it and which had clear relevance to publication activities. See D Erdos, 'Data Protection Confronts Freedom of Expression on the "New Media" Internet: The Stance of European Regulatory Authorities' (2015) 40 Eur L Rev 531, 550–51 and D Erdos, 'European Data Protection and Media Expression: Fundamentally Off Balance' (2016) 65 Int Comp L Quart 139.

129 Alongside ensuring compliance with stricter data subject rights, key changes for controllers including a new emphasis on their being able to demonstrate appropriate compliance with data protection (Regulation 2016/679, art 24), more formal duties to ensure data protection by design and default (ibid art 25) and obligations to undertake data protection impact assessments in situations of likely high risk (ibid art 35).

130 See generally Regulation 2016/679, ch III.

forgotten' encompassing an explicit requirement that controllers which have 'made the personal data [subject to erasure] public' also on request 'take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, personal data'.[131] It further tasks the new regulatory European Data Protection Board agency with issuing 'guidelines, recommendations and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services'.[132] In addition, it subjects processors to limited direct disciplining obligations for the first time.[133] Meanwhile, the new Regulation explicitly states that 'Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information'.[134] However, unlike the slightly revamped 'special expression derogation'[135], this new 'freedom of expression' clause fails to provide for any explicit *vires* for this task, beyond the 'other limited derogations' that are replicated from Directive 95/46 but in a more circumscribed formulation.[136]

Relevant CJEU and National Case Law

Notwithstanding that national data protection laws have almost never included provisions for reconciling themselves with freedom of expression other than in the area of journalistic/special expression, the CJEU in *Lindqvist* stressed that both 'authorities and courts of the Member States' were under a more wide-ranging obligation 'to make sure that they do not rely on an interpretation of [the Directive] which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality'.[137] Meanwhile, in *Satamedia* a Grand Chamber held that 'journalistic purposes' should be interpreted 'broadly'[138] so that, at least when processing related to 'documents which are in the public domain under national legislation', it encompassed activities whose object is 'the disclosure to the public of information, opinions or ideas'.[139] At the same time, it stressed that, even within this special area, derogations should apply 'only in so far as is *strictly* necessary'.[140]

131 Regulation 2016/679, art 17(1)(d).

132 ibid art 70(1)(d).

133 See, in particular, the obligations to record processing activities (ibid art 30(2)), appoint a data protection officer in certain circumstances (ibid art 7) and to notify the relevant controller of any data protection breach (ibid art 33(2)), as well as the new ability of regulatory Data Protection Authorities to enforce directly against processors including through obligating them 'to bring processing operations into compliance with the provisions of the Regulation' (ibid art 58(2)(d)).

134 ibid art 85(2). The reference to freedom of information here refers not to a right of public access to documents (as in the UK Freedom of Information Act 2000) but rather to the subset of freedom of expression explicitly related to the free flow of information as opposed to ideas.

135 ibid art 85(1).

136 These new provisions notably no longer provide for the possibility of derogating from the data protection principles in and of themselves.

137 *Lindqvist* at [87].

138 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* (C-73/07) EU:C:2008:727; [2008], at [56].

139 *Satamedia* at [61].

140 *Satamedia* at [56] (emphasis added).

To date, however, the CJEU has only specifically explored the data protection responsibility of intermediary publishers in *Google Spain* (2014) itself. Here, a Grand Chamber indicated that a generalized search engine indexing website content was a controller of the resulting processing but would not acquire positive duties except when its own activities were 'liable to affect' 'the fundamental rights to privacy and to the protection of personal data' 'significantly and additionally' compared with that of original publishers; even then, it would only have to act 'within the framework of its responsibilities, powers and capabilities'.[141] The Court construed[142] the concrete case at issue to be limited to a request to deindex specified links against the individual's name[143] and, in this context, found both of these thresholds met.[144] The Court also found that search engine indexing was not an exercise of special expression such as journalism,[145] that deindexing may be required even in cases where publication at source was entirely lawful[146] and that it was vital that 'effective and complete protection of data subjects' be ensured here.[147]

Turning to the national level, case law here remains rather diverse. A number of decisions involving evaluation or profiling sites of various sorts have mandated a very broad ambit of responsibility. For example, in the *Note2be.com* case, the teacher evaluation website being sued stated that they granted teachers a unilateral right to object to their evaluation by 'anonymous' users and that such objection would (presumably through the adoption of technical blocking measures) be honoured indefinitely. Notwithstanding the possibility of this strong but essentially *ex post* guarantee, however, the Cour d'appel de Paris prohibited this site processing the teachers' personal data on the basis that the service had not adopted *ex ante* measures to ensure that the data were collected fairly and were both relevant and accurate.[148] Meanwhile, the Rechtbank Utrecht judgment concerning a grandparent estrangement site expected this service itself to ensure that the named grandchildren and their parents were informed and gave their consent to this.[149] As this had not happened, processing of this data was prohibited.[150] Somewhat similarly, in the Polish doctor evaluation site case, the Naczelny Sąd Administracyjny emphasized that it

141 *Google Spain* at [38].

142 During the hearing it was clarified that the applicant was only demanding that 'information should no longer be displayed in the search results presented by the internet search engine operated by Google, when a search is made of his name and surnames' (C-131/12 *Google Spain (AG Opinion)* (2013) EU:C:2013:424 at [5]).

143 *Google Spain* at [62].

144 *Google Spain* at [88].

145 *Google Spain* at [85].

146 *Google Spain* at [62].

147 *Google Spain* at [38].

148 *Note2be.com Ltd, Mr SC v La Federation Syndicale Unitaire and Others*, 08/04727. The lower Tribunal de Grande Instance de Paris judgment, which was essentially upheld on this point, was explicit that expecting teachers who had never exercised their right to objection before to periodically monitor the site to potentially exercise this right imposed a disproportionate burden upon them. See *Note2be.com Ltd, Mr SC v La Federation Syndicale Unitaire and Others*, 08/51650.

149 ECLI:NL:RBUTR:2009:BJ1409 at [5.10].

150 ECLI:NL:RBUTR:2009:BJ1409 at [5.15]. It was clear that the strict analysis in this judgment was influenced by what it saw as the low value of the expression on the site coupled with its gross privacy infringement. If such factors had not been present then a different analysis may have presented itself under the principle of proportionality.

expected this service to proactively ensure that the transparency obligations to the named doctors were met.[151] On the other hand, turning back to the *Note2be.com* case, the Cour d'appel adopted a different analysis as regards the free-text user forum that was linked to, but distinguishable from, the structured evaluative portion of the site. In sum, while upholding the lower court's ruling that the teachers' personal data should also be prohibited there, it deleted (albeit without elaboration of its reasons) this court's requirement that the service adopt a mechanism of prior restraint or other (similarly) effective mechanism to achieve this.[152]

Ambit of responsibility issues have been analysed most extensively in relation to generalized search engines. Even prior to *Google Spain*, three French decisions (from 2010, 2012 and 2014) had explored aspects of this question. In the first, an individual sought to require Google to ensure that a pornographic video in which she appeared was not indexed against her name coupled with further specified terms linked to pornography. While acknowledging that it would be impossible for a search engine to carry out an *ex ante* review of the sites which it indexed, the Tribunal de Grande Instance de Montpellier found that Google was capable after generic notification of searching out the precise links in which the video appeared and should deindex accordingly.[153] The second and third cases respectively concerned requests that Google deindex certain specified links (also linked to pornography) against an individual's name and that it prohibit certain pejorative 'autosuggest' keywords being generated by the input of a natural person's name. Both claims were upheld.[154] Subsequent to *Google Spain* the number of cases seeking to hold search engines responsible under data protection has exponentially increased. Most have been limited to the same ambit as the CJEU construed *Google Spain* itself.[155] Nevertheless, some claims have, similarly to the first French case, directly sought a different and to an extent broader result. In particular, a few recent German, Italian and UK cases have explored whether an individual with a well-founded objection to the indexing of certain data can fix a search engine with wider preventative duties than simply deindexing specified individual links at one point in time. A complication arises from the fact that, in Germany, both individuals and the courts have conceptualized search engines' primary responsibilities here under that country's civil right of personality, with data protection often confined to a subsidiary role. In the first German case, decided by the Landgesricht Hamburg in November 2014, an individual sought to

151 I OSK 1480/14.

152 *Note2be.com Ltd, Mr SC v La Federation Syndicale Unitaire and Others*, 08/04727.

153 *Mme C v Google France and Google Inc* (2010). It appears that Mme C had consented to appearing in a published pornographic video but that it had then been placed on the internet without her further authorization.

154 See *Diana Z v Google* (2012) and *MX v Google and Google France* (Tribunal de commerce de Paris (First Chamber), 28 January 2014).

155 In fact, the regulatory decision under review in *Google Spain* (and in a number of linked cases under stay in Spain at the same time) was couched in the apparently broader language of requiring Google to 'withdraw the data from its index and to render future access to them impossible' (*Google Spain* (2014) at [22]). However, this was construed by the national court as having the same ambit as referenced by the CJEU and demanded by the data subject in this case; moreover, subsequent regulatory decisions in Spain have to date adopted more explicitly limited language. See ECLI:ES:AN:2014:5129 (*Costeja*) and generally M. Peguera, 'In the aftermath of Google Spain: how the 'right to be forgotten' is being shaped in Spain by courts and the Data Protection Authority' (2015) 23 Intl J L & Info Tech 325, 328.

prohibit Google from including 'snippets' of various pejorative and at least unproven information within nominative search results. Without requiring the subject to provide specific links to Google, the Court upheld this finding that an ongoing 'repetition hazard' existed as regards future breach of the applicant's rights and it was reasonable for Google to take measures against this.[156] In a second case, decided by the Landesgericht Heidelberg the following month, the data subjects objected to continued nominative indexing of information which not only accused them of racist attitudes and activities but also identified them in multiple ways, including by reference to their former residence. While some such links were deindexed by Google, this information was regularly reposted at the same website; as a result, the subject sought to prevent Google linking anywhere to the site in a nominative search. Although rejecting this, the Court held that Google had to ensure after notification that the actual information in question, and not just specific links, were permanently removed or filtered.[157] In December 2016, however, the Oberlandesgericht Karlsruhe overturned this ruling, finding that Google was only a 'indirect disturber' of the right to personality and that, since it was engaged in a socially desirable business model, the only duty reasonably to be expected of it was the deletion specifically violative links after notice.[158] This reasoning was also followed by the Landgericht Köln in a third case decided in August 2015, reasoning which was upheld by the Oberlandesgericht Köln in October 2016 with a further finding that a search engine only needed to act when the data subject provided evidence of a clear violation of the law.[159] In Italy, in the process of rejecting the notion that a search engine could be responsible under data protection for checking through an entire internet domain for inaccurate information, the Tribunale di Milano explicitly held that specific URLs must be provided before a search engine was fixed with responsibility here.[160]

156 Landgericht Hamburg, 7 November 2014, 324 0 660/12.

157 Landgericht Heidelberg, 9 December 2014, 2 O 162/13. As previously noted the Court left open whether the search engine could in principle claim the 'host' shield here (see above note 90) but was clear that such duties could apply irrespective of this as Google was only liable for the illegality of information after being notified of its illegality.

158 Oberlandesgericht Karlsruhe, 14 December 2016, 6 U 2/15. The Oberlandesgericht further held that the lower court had had no power to grant a remedy not requested by the data subject and, in light of the fact that they had moved residence, also reversed the finding that there was a substantive violation of law in any case. Interestingly, in contrast to the lower court decision, this judgment made absolutely no mention of European data protection as opposed to the civil right to personality. As noted above, this decision is currently being appealed to the Bundesgerichtshof.

159 See Landgericht Köln, 16 August 2016, O 14/14 and Oberlandesgericht Köln, 13 October 2016, 15 U 173/15. In light of the higher threshold it set out, the latter court also reversed the finding of a substantive violation of the law. Although the filtering issue was explicitly not explored, this threshold definition and substantive finding was upheld in Bundesgerichtshof, 27 February 2018 VI ZR 489/16, with this court being explicit that this did result in search engines having less responsibility here even that 'hosts'. Rather than focusing on Google's *prima facie* responsibilities as a 'controller', the court accepted and emphasized Google's contention that it had limited technical ability to check the legitimacy of data processing or do anything other than deindex entire pages. In some contrast, in the UK case of *NT1 NT2 v Google* (2008), the court appeared in principle open to considering whether it was feasible to require Google to comply with novel obligations such as adding a supplementary statement to indexed data (at [86]).

160 Tribunale di Milano, 21 November 2016 (10302/2016) (upholding in the process nominative deindexing of specific URLs linking to false information).

In contrast, the Tribunale di Spoleto ordered Google to nominatively deindex all articles on the internet making allegations against the data subject in relation to paedophilia (and harassment) without the URLs for these having been provided.[161] Turning finally to the UK, in *Mosley v Google Inc & Or*, the applicant sought to deploy the UK's transposition of the right to object[162] to require Google search engine to block access to his sensitive personal data[163] in the form of images of him engaging in private sexual activity. While conducting only an interlocutory review, the England and Wales High Court stated that '[t]he claimant's assertion that he has suffered substantial unwarranted distress is plainly capable of belief and, if so, founding the remedy which he seeks'.[164] The Court was undeterred by the fact that Mosley's claim both encompassed the blocking of data itself and was not confined to nominative searches.[165] In contrast, other cases have explicitly limited proactive deindexing obligations to nominative searches,[166] with at least a couple from Italy even explicitly interpreting this so as to exclude searches including a name alongside other terms, at least when input of these required some awareness related to the material being deindexed.[167] However, this latter interpretation was firmly rejected by the French Cour de cassation in a final judgment handed down on 14 February 2018.[168]

Finally, the Italian Corte di Cassazione *Google Video* judgment of 2013 held that, although data protection law did apply to this video-sharing service, it would only become a controller of the uploaded data after notification of the fact that the information was illegally published and it had failed to immediately remove it. In sum, despite holding that the intermediary 'host' shield was not directly applicable in a

161 Tribunale di Spoleto, 14 December 2016 (825/2016). This decision is under appeal (on both ambit of responsibility and substantive grounds).

162 UK, Data Protection Act 1998, s 10.

163 See above note 124.

164 *Mosley v Google Inc & Or* (2015) at [23]. Interesting, under French civil privacy law Mosley had obtained a similar remedy before the Tribunal de Grande Instance de Paris in 2013 requiring that Google block nine private sexual images albeit only for the limited period of this five years. See *Max Mosley v Google Inc and Google France*, 11/07970 (6 November 2013).

165 See, however, the *obiter* remarks made at [136] in *NT1, NT2 v Google* (2008) which appear in some tension with this.

166 See, for example, ECLI:NL:RBAM:2015:716 at [4.8] (rejecting deindexing under the term 'CEO KPMG') and ECLI:NL:RBDHA:2017:264 at [3.6] (rejecting the deindexing of five URLs on *inter alia* the basis that it had not been shown that the links in question appeared in a search against the data subjects' name).

167 See Tribunale de Milano, 17 May 2016 (5640/2016) and Tribunal di Milano, 21 November 2016 (10302/2016). In contrast, in a case published by the Tribunale di Perugia on 26 January 2016 (RG 6255/2014) the Court duly considered the claim from the data subject as regards a nominative search including a search term relevant to the linked information ('Massoneria' ie 'Masonry') although it weighed this as a factor against delisting on the basis that links via such terms would have less impact on the subject. In the event, the claim in question was rejected on the merits.

168 See *MX v Google* (Cour de Cassation (First Chamber), 14 February 2018) (ordering deindexing vis-à-vis all searches including the surname and first name of MX). Similarly, in March 2018, the Belgium Commission de la protection de la vie privée held that search engines should interpret nominative searches to cover any search including a name (ie irrespective if it contained additional keywords). See Commission de la protection de la vie privée, 'La Commission vie privée formule des recommandations à l'égard d'un moteur de recherche concernant le déréférencement d'URL's' (2018) <https://www.privacycommission.be/fr/news/la-commission-vie-privee-formule-des-recommandations-a-legard-dun-moteur-de-recherche> accessed 27 April 2018. This finding, however, has not (yet) resulted in court action.

data protection context,[169] the Court developed a cognate outcome through the ascription of a restrictive meaning to the term 'controller'. In so doing, it draw strongly on the Advocate-General's Opinion in *Google Spain* which, albeit in the somewhat different area of search engine indexing, conceptualized the issue as one of 'secondary liability' only, thereby enabling ready application of the intermediary shield case law by analogy.[170] However, this understanding was decisively rejected in *Google Spain* itself.[171]

TOWARDS A NEW SYNTHETIC APPROACH

General considerations

As can be seen in the descriptive analysis above, although codified data protection and intermediary shield law were originally conceived as self-contained and separate legal areas, intermediary publisher jurisprudence increasingly fuses these frameworks, while also emphasizing the need to ensure a proportionate balance between rights under general human rights law. Regulation 2016/679 bolsters this trend by including a gloss on the meaning of the Directive 2000/31's data protection clause,[172] a clause emphasizing the need to reconcile data protection with freedom of expression,[173] a new provision on the 'right to be forgotten' especially focused on publicly available communication services[174] and a new recital emphasizing that that data protection continues apply to services, which provide the means for even purely personal or household processing.[175] This general emphasis on augmenting positive duties within the context of competing rights and often also the engagement of the intermediary shields chime with two other proposed Digital Single Market initiatives which attempt in the areas of 'hate speech' and child protection[176] as well as copyright[177] to set out measures[178] to address some of the real harms associated with

169 See above note 45.

170 *Google Spain (AG Opinion)* at [46].

171 See above note 141.

172 Regulation 2016/679, art 2(4).

173 ibid art 85(1).

174 ibid art 17.

175 ibid recital 18.

176 European Commission, *Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities* (COM (2016) 287 final).

177 European Commission, *Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market* (COM (2016) 593 final).

178 The proposal on hate speech and child protection, which extends only to 'video-sharing platforms' (above n 176, 29), specifies that such positive measures shall consist of the following as appropriate: (i) defining and applying terms and conditions in these two areas, (ii) establishing and operating mechanisms for users to report or flag problematic content, (iii) explaining to users what effect has been given to such reporting and flagging, (iv) enabling users to rate content, (v) establishing and operating age verification systems in relation to content and (vi) providing parental content systems with respect to age-related content (above n 176, 29–30). Meanwhile the copyright proposal, which encompasses '[i]nformation society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users' (above n 177, 29) would require such services to take 'appropriate and proportionate' measures such as 'the use effective content recognition technologies' to implement agreements concluded with rightsholders or to the prevent the availability of works or other

certain intermediary publication activities. Unfortunately, however, case law specifying the responsibility of intermediary publishers as regard third-party personal data remains incomplete, fragmented and, in particular as regards those parts focused on the data protection law itself, inconsistent and sometimes unbalanced. Moreover, in significant contrast to the other Digital Single Market initiatives mentioned above, Regulation 2016/679 seeks only to clarify certain elements of the current *status quo* rather than engaging in anything like comprehensive legal reform. Given this, it is vital to bring more coherence and balance to the delimitation of ambit of responsibility here through a new and primarily interpretative synthesis of the three legal frameworks operating in this area. As argued and developed below, such a synthesis should have three dimensions. First, some overarching principles of interpretation need to be developed to reconcile the core ends that these three legal frameworks seek to pursue. Secondly, at a conceptual level, the various definitional concepts found within codified data protection and intermediary shield law should be fully deployed so that they all perform relevant work and none are excessively stretched such that they unduly dominate or colonize this space. Finally, these two dimensions must to be brought together in a final integrative dimension.

Looking first to the development of overarching principles, it is clear that the core ends of these three legal frameworks are in substantial tension. Thus, codified intermediary shield law is principally designed to make sure that certain intermediary publishers are not primarily liable for 'illegal acts initiated by others'[179] or, in this article's terms, for acts initiated by original publishers. Meanwhile, codified data protection law seeks to ensure that online services (including potentially intermediary publishers) are responsible for safeguarding individuals' privacy and related rights in so far as they 'alone or jointly with others, determin[e] the purposes and means of the processing of personal data'.[180] Finally, general human rights law aims to function as a backstop guarantee that specific legal provisions not only secure basic rights[181] but, more particularly, only impose limitations which respect the essence of those rights and are compatible with the overarching principle of proportionality.[182] In this context, and without downplaying defensive rights such as privacy which data protection is dedicated to vindicating, it must be recognized that intermediary publisher activity almost always constitutes a manifestation of freedom of expression,[183] as well the related freedom of conducting a business.[184] It is therefore necessary that these rights are not unduly impinged upon, an imperative that is also reflected in Regulation 2016/679's new freedom of expression clause, Article 85(1). These often competing ends may be synthesized or reconciled by the following three interlinked and overarching principles. First, that as an intermediary publisher exercises more

subject matter identified by rightsholders which fall outside such agreements and, further, that they provide the latter 'with adequate information on the functioning and development of the measures, as well as, where relevant, adequate report on the recognition and use of the works or other subject-matter' (above n 177, 29–30).

179 European Commission (COM (1998) 586 final) 27.

180 Regulation 2016/79, art 5(7) and Directive 95/46, art 2(d).

181 European Convention, art 1.

182 EU Charter, art 52 (1).

183 European Convention, art 10; EU Charter, art 11.

184 EU Charter, art 16.

autonomous control over processing, so the basis for it being subject to the various duties set out in codified data protection law becomes stronger and the legitimacy of deploying codified intermediary shield law to severely limit these is in contrast weaker. Nevertheless, and secondly, that even when such codified intermediary provisions are entirely inapplicable, some ambit of responsibility shields may remain necessary to safeguard freedom of expression and related rights. Thirdly, and also to avoid a disproportionate outcome, that some account must be taken of the divergent 'capacities' of even similarly situated intermediary publishers given potentially radical divergences in the level of their resourcing.

Turning next to the conceptual dimension, an attempt to ensure that each of the core definitional concepts within codified data protection and intermediary shield law are given due weight and that none are excessively stretched leads, as further developed and justified below, to the following taxonomy:

- 'Processor hosts', encompassing those which fall within the 'host' intermediary shield and outside the definition of 'controller' under data protection,
- 'Controller hosts', covering those who fall within the 'host' intermediary shield and also within the 'controller' definition under data protection and
- 'Independent intermediaries', comprising those who fall within the 'controller' definition under data protection and outside 'host' intermediary shield.

Turning to the final 'integrative dimension', it is important to recognize that the taxonomy above not only draws on concepts embedded within the relevant legal frameworks but also, in so doing, creates a structured spectrum of increasingly autonomous intermediary publishers. Given this, and in line with the first two principles included within the first dimension, the basic ambit of responsibility should be primarily structured according to, and increase along, this spectrum. Nevertheless, in light of the second and third principles above, the ambits of responsibility arising from this structure must also be reconciled with freedom of expression and, moreover, the detailed elaboration of duties must allow for account to be taken of the divergent resource capacity of even otherwise similarly situated intermediary publishers.

The rest of this section provides a further specification of, and justification for, this synthetic approach looking both at the types of intermediary publisher included within the three categories as well as the ambit of responsibility that should apply to them in light of the legal frameworks that applying in the new era of Regulation 2016/679.

Processor Hosts

This first category encompasses an important, albeit increasingly less central, subset of intermediary publishers whose publication activity takes place under the direct instruction of an another original (or indeed intermediary) publisher. Examples include not only website but also some forms of blog maintenance. Since these actors exercise no habitual autonomy in their information processing, they should, as was stated in the Spanish Google Blogger judgment, be characterized not as 'controllers' but

only as 'processors'.[185] Processors are not directly responsible for ensuring adherence to substantive data protection standards, a position which is maintained in Regulation 2016/679. However, while in the era of Directive 95/46 this remained a matter of national discretion,[186] the new Regulation does require that regulators (and possibly, by implication, also courts) are empowered to order processors 'to bring processing into compliance with the provisions of the Regulation, where appropriate, in a specified manner and within a specified period'.[187] It also stipulates that processors compile records, to be supplied to regulators on request, including the name and contact details of all controllers (who, in this context, will generally be natural persons) on behalf of whom they are processing.[188] Notwithstanding that they may provide facilities such as tool integration which go beyond the 'storage' and 'communication' operations defined in intermediary shield law, it was clearly the intention that these kind of services should in principle also be protected by the 'host' shield.[189] Moreover, especially given Regulation 2016/679's new gloss in this regard, it would be perverse to deploy Directive 2000/31's data protection clause to render such a result exceptionally inapplicable in a data protection context. Nevertheless, given Directive 2000/31's explicit carve-outs both for injunctive relief[190] and for any obligation placed on hosts to 'communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements',[191] deployment of this shield makes little practical difference here.

Turning to an overarching rights analysis, that compliance with substantive data protection is not the direct responsibility of such actors flows appropriately from the essentially dependent nature of their activities. At the same time, the possibility of fixing them with limited injunctive duties reflects the fact that this may be necessary in particular cases to effectively vindicate the right to data protection. However, to respect the freedom of expression rights of original publishers on whom processor hosts are dependent, any such injunctions should remain targeted and regulators and/or courts should in any case consider whether redress can reasonably be pursued directly, either entirely or in part, with original publishers themselves. While truly anonymous publication poses a formidable barrier to such direct redress, it is an integral part of freedom of expression (and further has a clear link to the right of privacy and therefore data protection itself). Thus, as the European Court of Human Rights has elucidated it has 'long been a means of avoiding reprisals or unwanted attention' and 'is capable of promoting the free flow of ideas and information in an

185 See above n 37.

186 Subject to the never tested potential for the recognition of data protection as an EU fundamental right to require courts to craft such a remedy in certain contexts.

187 Regulation 2016/679, art 58(2)(d).

188 Regulation 2016/679, art 30(2)-(4). Under art 30(5) such record keeping is not required of processors employing less than 250 persons unless the processing is not occasional, includes sensitive data or is likely to result in a risk to the rights and freedoms of data subjects. However, given these many caveats, it is unclear whether any intermediary publisher could be sure of satisfying these exemptions.

189 See in particular above n 58.

190 Directive 2000/31, art 14(2).

191 Directive 2000/31, art 15(2).

important manner, including, notably, on the Internet'.[192] Requiring processor hosts to keep and supply on request pinpoint name and address records for all original publishers implies that all such autonomous publishers, even if only publishing innocuous personal data, would need to be subject to authentication and run the risk of their details later being handed over to a state authority. This could be considered to violate the essence of the right to anonymous expression and, in any case, would certainly constitute a disproportionate limitation on it in particular cases. Member States should therefore provide for a derogation from this provision under Article 85(1) of Regulation 2016/679 and, in the absence of this, courts should also recognize a similar limitation directly under Article 85(1) and primary law including the EU Charter. At the same time, in light of the 'ease, scope and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed',[193] it is vital to ensure the effective redress of legal harms here. Given this, the use of any such derogation should be made subject to appropriate safeguards such as requiring that these processors after notice block or erase manifestly illegal content without waiting to be fixed with injunctive relief.

Controller Hosts

Original publishers increasingly upload and maintain content on services that do not limit their publication-related processing to those under the direct instruction of original publishers but rather fuse this to additional acts that they themselves determine such as combining, aligning and organizing content to ensure its ready retrievability and/or to push it to end users.[194] While almost all such services undertake this kind of additional processing on an *ex post* basis, some also seek *ex ante* to systematically pull content into their services, as is the case with the upload of user-generated street-level images in the case of Google Maps. Other clear examples of 'controller hosts' include video-sharing sites such as YouTube and social networking sites such as Facebook. In light of their autonomous decision-making, courts have rightly held that these entities are 'controllers' under European data protection. Although it would sometimes be possible to granularize the nature of such control down to the particular types of additional processing they engage in, the fused nature of these services' operations mean that this will often only make a marginal difference to what is required to ensure legal compliance.[195] Nevertheless, in light of their ongoing relationship with original publishers, it is important to recognize that these actors are controllers of a special type. Reflecting this, and albeit through adopting a very flexible approach to its terms, courts have also recognized that such services can benefit from the 'host' immunity in intermediary shield law. Clearly, this reveals considerable tension between conceptualization of the concept of agency in these two bodies of law. In rough terms, while data protection sees the exercise of even generic control

192 *Delfi v Estonia* App no 64569 (ECtHR, 16 June 2015) at [147].

193 *Delfi v Estonia* (2015) at [147].

194 Notably through autonomous search functionality, content 'feeds' and automated recommendations.

195 Such an approach would also entail that in relation to their less autonomous processing, these services are acting as the data 'processors' of original publishers. This would *inter alia* trigger the default rules requiring a recording of such publishers' names, address and other details, the problems as regards which have already been dealt with above.

as sufficient agency to trigger 'controller' status, intermediary law requires that knowledge and/or control over information be very specific before 'host' immunity is lost.

Going forward, these divergent understandings should be synthesized through crafting a stable and balanced understanding of what it means to be both an intermediary host and a personal data controller. It is argued that intermediary shield law already provides the basis for this by recognizing, first, that 'hosts' can never be fixed with liability for particular illegalities on their services absent knowledge of this,[196] but that secondly they can be required to comply with such 'duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities'.[197] For personal data controllers, these duties are in principle specified within codified data protection law. In light of the first stipulation, it is imperative that data protection law be disapplied to the extent that it fixes host controllers with direct *ex ante* liability for illegalities arising from the processing of personal data on their site.[198] On the other hand, however, those parts of data protection law which set out more general duties of care to assess the organization of processing operations as a whole and which additionally require controllers to vindicate data subject rights *ex post* can and therefore should be applied alongside this qualified shield. Thus, turning to the first of these, Regulation 2016/679 requires that 'where proportionate' such services adopt 'appropriate data protection policies'[199] aimed at ensuring that the data uploaded into their services does not violate data protection standards. Given the peculiar nature of their processing, it would generally be reasonable for these services to argue that they are 'joint controllers' with these original publishers. If so, provisions here could be limited to a transparent arrangement detailing the responsibilities of users themselves to ensure that the material initially uploaded on the service was lawful under data protection.[200] At the least, therefore, such services should have 'clear and prominent policies for users [original publishers] about acceptable and non-acceptable posts'.[201] In addition, 'controller hosts' would need to adopt 'appropriate technical and organizational measures'[202] to guard against their own combining, aligning and organizing of

196 Directive 2000/31, art 14(1).

197 Directive 2000/31, recital 48.

198 Directive 2000/31, art 14(1). Absolute liability for any and all illegalities would also require precisely the type of general monitoring prohibited by art 15.

199 Regulation 2016/679, art 24(2).

200 Regulation 2016/679, art 26. Such an arrangement would be without prejudice to a data subject's right to exercise their rights *ex post* against either party (Regulation 2016/679, art 26(3)). In addition, this arrangement would technically trigger record-keeping requirements cognate to those of data 'processors' (Regulation 2016/679, art 30(1)(a)), the problems and potential solutions to which have already been dealt with in the previous subsection.

201 United Kingdom, Information Commissioner's Office, *Social networking and online forums—when does the DPA apply?* (n.d./2013) <https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf> accessed 29 April 2018. See in a similar vein European Union, Article 29 Working Party, *Opinion 5/2009 on Online Social Networking* (2009) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> accessed 29 April 2018, which additionally sought to lay down overly restrictive and prescriptive stipulations here, namely, that '[u]sers should be advised by SNS [social networking sites] that pictures or information about other individuals, should only be uploaded with the individual's consent' (12).

202 Regulation 2016/679, art 24.

content itself posing a systemic threat to data protection. In particular, insofar as a service's own processing is 'likely to result in a high risk to the rights and freedoms of natural persons'[203] the controller would need to carry out a data protection impact assessment prior to rolling this out.[204] The implementation of facial recognition technology presents a clear example of where this would likely be triggered. Meanwhile, requirements to vindicate rights *ex post*[205] may on occasion require 'controller hosts', following data subject contact regarding a potential data protection concern, to take reasonable steps to detect the precise processing at issue, undertake a *bona fide* assessment of its legality and adopt continuing measures to prevent the repetition of specific illegalities. In principle, however, such responsibilities are not inconsistent with the duties of care logic in the host intermediary shield, have already been recognized in a number of cases which give close attention to the structure of European data protection[206] and need not necessarily be interpreted in a way which disproportionately impacts freedom of expression. Thus, when a data subject sustains a *bona fide* objection to processing, Regulation 2016/679 in principle requires that the controller 'no longer process the personal data'.[207] As suggested by the interpretation of the cognate Directive 95/46 provision[208] in *Mosley v Google*,[209] this could extend to the adoption of ongoing measures to prevent such processing in future which, given its clearly specified nature, should also not *ipso facto* fall foul of the prohibition on general monitoring[210] set out intermediary shield law. Nevertheless, a requirement to adopt ongoing measures would never apply where the controller 'demonstrates compelling legitimate grounds' which override this.[211] Given the current state of technology, such a threshold would ordinarily be met as regards controllers with limited resources and no existing capacity so to act. In contrast, it should not be satisfied as regards seriously prejudicial content such as intimate images where 'it is common ground that existing technology permits [the controller], without disproportionate effort or expense, to block access to individual images, as it can do with child sexual abuse imagery'.[212] Meanwhile, the Regulation's new 'right to be

203 Regulation 2016/679, arts 24(1) and 25.

204 Such an assessment would encompass 'a systematic description of the envisaged processing', an assessment of both its 'necessity and proportionality' and 'the risks to the rights and freedoms of data subjects' and finally 'the measures envisaged to address the risks . . . taking into account the rights and legitimate interests of data subjects and other persons concerned' (Regulation 2016/679, art 35(7)). In the intermediary publisher situations, the relevant 'legitimate interests' would often relate to the enjoyment of fundamental rights and could be wide-ranging including not those of the company and data subject but also potentially original publishers and the end users of information.

205 Principally, the rights to erasure/to be forgotten (Regulation 2016/679, art 17) and to object to processing (Regulation 2016/679, art 28) coupled with the residual right to a restriction of processing in certain circumstances (Regulation 2016/679, art 18). An attempt may be made also to be provided *ex post* with information on processing under the right of access (Regulation 2016/679, art 15).

206 For example, *Mme C v Google France and Google Inc* and *Mosley v Google Inc & Or*.

207 Regulation 2016/679, art 21(1).

208 Directive 95/46, art 14(a).

209 Albeit in relation to a generalized search engine rather than the 'controller hosts' dealt within in this subsection. However, the interlocutory decision of *AY v Facebook* come to a similar finding, albeit on the basis of a much more truncated analysis.

210 Directive 2000/31, art 15.

211 Directive 2000/31, art 21 (1).

212 *Mosley v Google Inc & Or* (2015) at [52].

forgotten' empowers data subjects to require that controllers subject to a *bona fide* erasure demand who have made the relevant data public 'take *reasonable* steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data'.[213] Although undoubtedly both novel and challenging, the 'reasonable' qualification enables a similarly nuanced and proportionate interpretation. Some other default *ex post* rights, however, do have much more potential to disproportionately impact freedom of expression. For example, absent the subject presenting evidence which at least casts doubt on the accuracy of certain data, it may be impossible for a 'controller host' to come to a clear determination as to whether it should be removed for inaccuracy. However, by default, a controller under Regulation 2016/679 would not only have this responsibility but would, in addition, have to suspend publication of the information in the interim.[214] Even more ominously, such an entity would be required by default to provide the data subject with any information available as to the source of data,[215] a provision which could threaten anonymous speech even more seriously than the record-keeping requirements outlined in the previous subsection. Given this, Member States should explicitly provide for necessary and proportionate limitations on such these rights,[216] while still ensuring the essence of these rights to transparency and rectification are preserved.[217] In the absence of this, courts would need to adopt similar derogations directly as provided for in both Article 85(1) of the Regulation and also primary law such as the EU Charter.

Independent intermediaries

A final and also increasingly important category of intermediary publisher comprises those who, although 'intermediaries' in the broad sense that they perform processing activity directly linked to the activity of an 'original' publisher, carry out their activities so independently as to fall outside even a broad construction of the codified host intermediary shield (and indeed the other intermediary shields set out in Directive 2000/31). Such independence may arise simply from a service lacking any express relationship with these original publishers and thus any firm basis to demonstrate that they are operating at their 'request'.[218] Thus, despite valiant attempts by some courts to shoehorn this activity into the 'host'[219] intermediary shield, it is more logical to hold that a generalized search engine lacks the necessary *de jure* connection with the sites that it indexes.[220] Such an independence of processing is even clearer

213 Regulation 2016/679, art 17(2) (emphasis added).

214 Regulation 2016/679, art 18(1)(a).

215 Regulation 2016/679, art 15(1)(g).

216 Such derogations are permissible not only by implication under art 85(1) but also explicitly under art 23(1)(i) and, as regards journalistic/special expression, also in art 85(2).

217 Both are expressly recognized within the fundamental right to data protection set out in art 8 of the EU Charter.

218 Directive 2000/31, art 14(1).

219 See, for example, *Diana Z v Google* at note 89.

220 Such a conclusion was most crisply stated (albeit not in a personal data context) in *Metropolitan International Schools v Designtechnica Corpn* as regards the Google: '[T]he United Kingdom government [and Directive 2000/31] has so far taken the view that it is unnecessary or inappropriate to extend

in the case of services which, although obtaining raw data from original publishers, are predicated on systematically 'optimizing' and 'promoting' very particular types of personal data, thereby failing to adopt even the semblance of a 'neutral position'[221] here. Examples of such services include the highly systematized parts of an evaluation site, as well as specialized search engines which actively target 'specific types of personally identifiable information, such as social security numbers, credit card numbers, telephone numbers and email addresses'.[222] The latter services additionally lack an express relationship with the original publishers.

Given that they fall outside the type of intermediary services protected by Directive 2000/31, codified EU law would indicate that, when processing personal data, such independent intermediaries should simply fulfil all the controller obligations as set down in the European data protection law. As noted in the 'European Data Protection's Legislative Scheme' subsection above, this would entail a comprehensive *ex ante* and *ex post* responsibility for ensuring that data met all substantive benchmarks including, for example, as regards data accuracy and restrictions around the processing of sensitive personal data. In light of their generally automated reliance on content from other 'original' publishers, however, it seems clear that such a wide ambit of responsibility would burden these operators with similar difficulties to that which prompted the qualified intermediary shield to be codified for 'hosts'. Given this, the failure to provide for any shield here would likely constitute a disproportionate burden on freedom of expression and cognate rights.[223] On the other hand, however, not only must the existing conceptual definitions found in the law be accorded due respect, but the broader rationale for ascribing greater responsibility to more autonomous activity must also be recognized.[224]

protection expressly to search engines. It would not be appropriate, therefore, for me to proceed as though there were a comparable statute in effect in this jurisdiction. I think that, for the third defendant to be classified as or deemed a "host", statutory intervention would be needed' (at [112]). Since such a service is not storing data 'for the sole purpose of making more efficient the information's onward transmission' (Directive 2000/31, art 13(1)) but rather is manifestly processing to create its own search service (ie engaging in a 'separate exploitation of the information' (COM (1998) 586 final, 29)) court decisions (see above notes 83 and 84) suggesting that the caching shield could be engaged here are even more implausible.

221 *L'Oréal* at [116].

222 European Union, Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines* (2008), 13 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> accessed 30 April 2018.

223 In light of the significant challenges of lawfully managing large amounts of content online, recent case law has even proved willing to grant online news archives a limit on their ambit of responsibility despite the fact that the data in question originates from themselves rather than from other original publishers. See Spain, Tribunal Supremo, Sala de lo Civil, ECLI:ES:TS:2015:4132 (15 October 2015).

224 It must also be noted that the rationale for the specific e-Commerce shields was primarily economic and only secondarily rights-based (see above notes 48 and 49). Moreover, it may be credibly argued that, at least when protective rights are seriously threatened online, these shields may even be in tension with Member States' core duties to ensure respect for private life as set out under the European Convention on Human Rights. These issues have been explored by the European Court of Human Rights in a series of cases. See in particular the Grand Chamber decision of *Delfi v Estonia* (2015) as well as initial decision of *Delfi v Estonia* (ECtHR, 10 October 2013) and the later case of *Magyar Tartalomszolgáatatók Egyesülete & Index.hu zrt v Hungary* App no 22947/13 (ECtHR, 2 February 2016).

Albeit with disappointingly little explication of its rationale,[225] the CJEU addressed such dilemmas specifically as regards generalized search engines in its seminal *Google Spain* judgment. First, it held that positive obligations here would only be triggered insofar as the processing was 'liable to affect significantly, and additionally compared with that of the [original] publishers . . . the fundamental rights to privacy and to the protection of personal data'. Secondly, it argued that the resulting duties would need to be determined 'within the framework' of the service's 'responsibilities, powers and capabilities', while also emphasizing that the ultimate aim was to ensure 'that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved'.[226] Although a useful starting point, these determinations remain vague and, therefore, require considerable further specification. As regards the first limitation, it is unclear if this rests on the particularities of a generalized search engine, such as its especially strong reliance on output wholly extraneous from it (ie websites on the internet) and/or its lack of explicit optimization and promotion of particular categories of personal data, or if it also extends to independent intermediaries which lack such features. This issue may anyway have little practical significance since those later services such as evaluation sites and specialized search engines almost invariably pursue activity which are at least 'liable' to significantly and additionally impact data subjects. Moreover, it is also crucial to recognize that, although *Google Spain* focused on nominative indexing, such activity should not only be construed broadly[227] but is in any case but one example of processing with a sufficiently additionally impactful potential to trigger controller responsibilities even in cases when this threshold does apply.[228] Thus, in the first place, enabling a search by reference to a name in combination with other information about an individual would, at least if it is widely known[229] and/or suggested by a search engine's autocomplete functioning, be liable to have a significant and additional impact on the subject. Non-nominative examples of processing clearly liable to have significant and additional impact include indexing by reference to an individual image or another obvious non-nominative identifier such as a personal telephone number. Furthermore, the regulation of processing factually undertaken by such an independent intermediary which does not meet this threshold must also be determined; in this regard, it would seem important that regulators (and ultimately courts) are still able to issue specific injunctive relief here, thereby treating these actors as quasi-processors in this context.[230]

225 Most strikingly, the CJEU failed to explicitly acknowledge that freedom of expression was engaged. See more generally Stefan Kulk and Frederik Borgesius, 'Google Spain v González: Did the Court Forget about Freedom of Expression?' (2014) 5 EJRR 389.

226 *Google Spain* at [38].

227 See above note 168.

228 *Google Spain* at [80].

229 The combination of an individual's name with his or her locality of residence and/or work would be a particularly clear example of this.

230 This would ensure, for example, that data subjects could apply for an injunction to obtain even in relation to generalized search engines a complete blocking of very seriously illegal information the continued distribution of which was causing serious damage (eg revenge pornography). Such a remedy might be particularly important in cases where it was impossible to pursue the original publisher in relation to this due, for example, to their being untraceable or out of jurisdiction.

Turning to the second limitation concerning the intermediary's 'responsibilities, powers and capabilities',[231] the test here essentially requires a balance of rights and interests to be struck between a service's operational needs[232] and the importance of ensuring that the guarantees laid down in European data protection are given 'full effect'.[233] In this regard, and paralleling the structural relationship between data protection and the codified intermediary shields explored above, the more a service pursues essentially autonomous self-directed processing, the more it should be expected to adjust this to the data protection framework.[234] In this regard, there is even substantial divergence within the category of independent intermediaries. Thus, aside from lacking an express relationship with these actors, a generalized search engine sits in at least as dependent a relationship with original publishers as that of many 'controller hosts'. As a result, it would be reasonable in the interests of freedom of expression to provide for an essentially cognate limitation of its ambit of responsibility.[235] If this is accepted then, mirroring the situation set out in the 'Specification of Responsibility under European Data Protection' subsection above, generalized search engines would be principally responsible for vindicating data subject's rights *ex post*. In addition, however, they would also need to adopt 'appropriate data protection policies'[236] as 'proportionate' to proactively guard against clear, systematic violations of the law. For example, such a service should be expected to take steps to ensure that terms linking a data subject with highly intimate and pejorative subject matter are not suggested via autocompletion technology without a check having been undertaken to ensure that this is plausibly legally justifiable. Similarly, if a search engine was put on constructive notice that a certain website was fundamentally orientated towards the publication of seriously and clearly illegal content (eg revenge pornography), it should adopt protective measures against this such as ensuring that relevant links are placed very low in search results or even through undertaking a legal check prior to indexing. On the other hand, however, services that are predicated on autonomously processing specific types of personal data in a particular way should be expected to assume a greater level of responsibility as regards its legality.

231 *Google Spain* at [38].

232 This is notwithstanding the judgment's apparent reference to not just one but three elements, namely, 'responsibilities, powers and capabilities'. Thus, the responsibilities of an independent intermediary are, at least as set down in codified law, that of a full controller and their powers are at least in a formal sense almost never circumscribed (ie no external entity is compelling Google to run a search engine or forced Note2be.com to run an evaluation site). Ultimately, therefore, the issue boils down to determining the capabilities which can reasonably be expected of a service given the need to balance operational needs/desiderata against data protection.

233 *Google Spain* at [38].

234 If this fundamental point, which is hard-baked into the EU legislative scheme, is ignored or minimized then new algorithmic services such as search engines will be granted an incoherent degree of latitude under law. This appears to be epitomized in recent German case law as referenced in footnote 159.

235 Thus, notwithstanding it not being explicitly provided for in codified European data protection law, treating search engines as akin to 'hosts' should not be seen as fundamentally incompatible with European data protection, while treating them as 'mere conduits' or even 'cachers' would so undermine its rationale (including the *Google Spain* decision) as to violate the principle of remedial effectiveness within EU law. However, rather than over-stretching the logic of the 'host' shield itself (see above note 89), such a shield should either be found in an explicit statutory provision (see above note 104) or be based on general human rights law.

236 Regulation 2016/679, art 24(2).

For example, such services should not be exempted from the requirement to publish, in an easily accessible form, transparency information specifying the purposes of processing, the categories of personal data, the legitimate interests pursued (or other legal basis for processing), the rights of data subjects to exercise their *ex ante* rights and the right to lodge a complaint with a regulator.[237] Nevertheless, given that even these publishing services principally depend on the automated processing of large qualities of personal data sourced from others, their right to freedom of expression would likely be unduly infringed unless they benefited from some limitation on their ambit of responsibility under data protection.[238] Thus, rather than being directly responsible for all inputted data, it would be reasonable for an evaluation site that had clearly and conspicuously[239] informed users of policies requiring them not to upload data which is inaccurate[240] or sensitive data which lacks a legal basis to be published[241] to rely initially on an expectation that users will comply with this. At the same time, such a service should still be responsible for ensuring that any processing which it positively intended was legitimate,[242] that subject rights were honoured *ex post*, that violations of relevant standards were policed (eg by suspending accounts of users in repeated violation) and that any accidental but systematic illegalities (eg the widespread upload of sensitive data without a legal base) were robustly addressed. A specialized search engine targeting specific types of personal data such as telephone numbers and email addresses should similarly be able to presumptively rely on the accuracy and initial legitimacy of data sourced from reputable original publishers elsewhere on the web. Nevertheless, again, such services should still be responsible for publishing basic transparency information, ensuring that the intended additional processing making the data more accessible and retrievable is itself lawful, that subject rights are honoured *ex post* and that any accidental but systematic legal issues are dealt with (eg by ceasing to index data from sites with a track record of sourcing information illegitimately). More detailed elaboration of such duties would need to take into account the size and resourcing of different actors, with more

237 Regulation 2016/679, art 14(5)(b).

238 Thus, a number of profiling and evaluation cases at national level appear to have incorrectly proceeded on the basis that controller duties should simply apply in full here. For possible examples see above notes 148, 149 and 151. Similarly, the Article 29 Working Party appears to have been too hasty in finding that where a search engine performs 'value-added operations linked to characteristics or types of personal data on the information they process . . . the search engine provider is fully responsible under data protection laws for the resulting content related to the processing of personal data' (European Union, Article 29 Working Party, *Opinion 1/2008*, 14).

239 These additional conditions are critical given widespread evidence that online policies which are not explicitly brought to the attention of users and/or which are drafted in dense and obscure language are routinely ignored. See, for example, J Obar and A Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2016) TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy <http://dx.doi.org/10.2139/ssrn.2757465> accessed 29 April 2018.

240 Regulation 2016/679, art 5(1)(d).

241 Regulation 2016/679, art 9.

242 In some cases, the whole design of a profiling or evaluation site has been found to be illegitimate. For relevant examples see cases cited at notes 41 and 42. Another clear example of such processing would be a specialized search engine deliberately targeting credit card numbers (cf European Union, Article 29 Working Party, *Opinion 1/2008*, 13).

formalized 'technical and organizational measures'[243] being expected of those who have greater capacities. Nevertheless, a basic failure to abide by these minimum standards should be recognized as being always incompatible with the service's overarching responsibility as an independent data controller.[244]

As can be seen, the CJEU's *Google Spain* dicta in this area remain rather unclear, both in terms of their reach and in terms of their application to particular circumstances. The qualifications it sets down also sit in tension with the provisions of European data protection as currently codified. The question therefore arises as to whether, and if so, how Member States might legislatively address these issues through Article 85(1) of the new Regulation, albeit bearing in mind that any implied *vires* beyond use of the other limited derogations[245] would need to be interpreted narrowly and strictly.[246] One possibility is that Member States should simply enact that European data protection 'shall not apply where this will be in violation of the freedom of information and expression'. Such a restriction was found in the law of at least one EU State[247] during the era of Directive 95/46 and could constitute a valuable backstop defence. However, since the entirety of data protection sits in tension with freedom of expression,[248] provisions such as these run the risk destabilizing this regime across the board. Any application to particular circumstances is also likely to remain rather opaque and unpredictable. Given this, provisions directly targeted to independent intermediaries remain critical. Thus, Member States could legislate a specific shield for information location tools such as generalized search engines broadly based on that of the existing shield for 'controller hosts'. More generally, they could also explicitly stipulate that any service engaged in publication-related processing directly linked to initial publication performed by others[249] benefits from the right to freedom of expression and should only be subject to such an ambit of responsibility as can reasonably be expected of them given the need to achieve a balance between their operational needs and the right to the protection of personal data. Beyond this, independent intermediaries should also be covered by the freedom of expression limits to certain *ex post* data subject rights outlined in the 'Specification of Responsibility under European Data Protection' subsection above. Nevertheless, it must be recognized that the meaning even of these directly targeted provisions would remain rather uncertain. However, this may be the inevitable result of the existing European *acquis* coupled with the gestational nature of the issues which are

243 Regulation 2016/679, art 24(1).

244 Regulation 2016/679, art 24.

245 Since these other limited derogations fail to extend to the material definitions of 'controller' and 'processor' or even allow for a limit on the data protection principles, any overarching imitation on the ambit of responsibility of particular types of such actor would seem to necessarily depend on the use of such implied *vires*.

246 Such an approach would mirror the construction and interpretation of implied terms and licenses within private contractual law.

247 Denmark, Compiled Version of the Act on Processing of Personal Data 2000, s 2(2).

248 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, 145.

249 In other words, publication intermediaries in the broad sense of this article although often falling outside the specific shields set out in Directive 2000/31.

emerging in this rapidly evolving space. Over time, further specificity should be provided through interpretations by courts and regulators, especially as assembled in the new European Data Protection Board.[250]

CONCLUSIONS

The ever-increasing digitization of our lives has resulted in dramatically more and more varied types of information about identified or identifiable individuals being published online, often without their consent and with serious implications for the privacy and related rights which European data protection law is dedicated to uphold. While original publishers are the initial and immediate cause of online publication of third-party personal data, intermediary publishers are not only contributory to this but increasingly engage in further (semi-)autonomous processing such as organizing or promoting such content. This factor, alongside the general impracticability of pursuing myriad and sometimes anonymous original publishers, has resulted in an increasing focus on the responsibilities of intermediary publishers in this area. While subjecting these actors to full default data protection 'controller' duties would bolster the position of third-party data subjects, it is liable to seriously conflict with freedom of expression (as well as related rights such as the right to conduct a business). Such potential conflict arises not just from data protection's substantive standards, but also from its assumption that the controllers' ambit of legal responsibility will encompass a comprehensive *ex ante* and *ex post* discipline over data processing. Given that substantive tensions have already been addressed in related work, this article has focused exclusively on the latter dimension through both a descriptive and normative interpretative analysis.

As regards the descriptive analysis of existing pan-EU and national legal frameworks and case law, it has been found that many types of intermediary publisher have been found to be 'controllers' under codified data protection and also to benefit from the qualified 'host' shield under codified intermediary law (or, in a few cases, a generally cognate shield established at national level for information location tool services). Meanwhile, much of this jurisprudence has also highlighted the role of the general human rights framework here, a focus which generally remains present even in cases where one or other of the codified frameworks has not been found applicable. This somewhat disjoined triangular situation has resulted in the specification of the responsibilities of various sorts of intermediary publisher often lacking consistency and sometimes also balance.

Although it would be best to address these problems through careful and comprehensive legal reform, Regulation 2016/679 provides only a gloss on the erstwhile *status quo* and a new legal initiative appears unlikely. Given that, this article has sought greater consistency and balance through a new synthetic interpretative approach

250 The latter body not only has an explicit obligation to issues 'guidelines, recommendations, and best practices' concerning the new 'right to be forgotten' (Regulation 2016/679, art 70(1)(d)), but also has a much more wide-ranging duty to 'ensure the consistent application' of the Regulation (Regulation 2016/679, art 70(1)).

developed along three dimensions—'principles', 'concepts' and finally 'integration'. Turning to the first of these, a reconciliation of the generally competing ends of these three frameworks leads to three interlinked principles: (i) that as an intermediary publisher exercises more autonomy over processing, so the basis for it being subject to the duties set out in codified data protection law becomes stronger and the legitimacy of deploying codified intermediary shield law to severely limit is accordingly weaker, (ii) but even when the codified shields are entirely inapplicable, some ambit of responsibility shields may remain necessary to protect freedom of expression and related rights and (iii) for similar reasons, some account must also be taken of the divergent capacities of even similarly situated intermediary publishers given potentially radical divergences in the level of their resourcing. Meanwhile, at a conceptual level, ensuring that the various definitional concepts embedded within codified data protection and intermediary shield law are given due weight and that none are over-stretched so as to unduly colonize this space leads to the following tripartite taxonomy: (i) intermediary publishers which are not only intermediary 'hosts' but also only data protection 'processors' (processor hosts), (ii) those which are 'hosts' but are also data 'controllers' (controller hosts) and (iii) those which are 'controllers' and are not 'hosts' (independent intermediaries). Finally, it is necessary to integrate these dimensions into a comprehensive interpretative approach. In this regard, it is vital to recognize that the taxonomy above not only adopts concepts embedded in the current codified frameworks but also sets out a structured spectrum of increasingly autonomous intermediary publishers. In light of this, and in line with the first two overarching principles, the basic ambit of responsibility should be primarily determined by, and increase along, this spectrum. Nevertheless, in light of the second and third principles above, the ambits of responsibility arising from this structure must be reconciled with freedom of expression and, moreover, the detailed elaboration of duties arising from it must enable account to be taken of the divergent resource capacity of even similarly situated actors. Through a careful analysis of these three frameworks and especially Regulation 2016/679, the penultimate section of this article provided an indication of how such an integrative synthetic approach could be achieved.

Ultimately, however, attempting a synthetic interpretation of these three often radically diverging legal frameworks can only go so far in bringing more coherence and balance to the law. Significant uncertainties undoubtedly will remain. Given this, some may argue that freedom of expression and cognate rights should lead to an even broader and deeper interpretation of both the codified and uncodified intermediary shields so as to largely or completely disable data protection responsibility here. Such a result, however, would fundamentally undermine Europe's commitment to a 'high level'[251] of data protection in this area, a result which would be particularly problematic given that technological developments guarantee that intermediary publishers will exert ever more impact on people's lives in the future. In lieu of this, both the courts and the regulators (including via the new European Data Protection

251 Regulation 2016/679, recital 7.

Board) should address these uncertainties through the production of high-quality and specific guidance over time. Even this, however, will far from eliminate all difficulties. Ultimately, however, that may be the price of seeking to vindicate competing laws and rights in the context of a very imperfect EU *acquis* and a very challenging socio-technological setting.