The road to responsibilities: new attitudes towards Internet intermediaries

Mac Síthigh, D. (2020). The road to responsibilities: new attitudes towards Internet intermediaries. *Information and Communications Technology Law*, *29*(1), 1-21. https://doi.org/10.1080/13600834.2020.1677369

Published in:
Information and Communications Technology Law

Document Version:
Peer reviewed version

The road to responsibilities: new attitudes towards Internet intermediaries

Daithí Mac Síthigh*

October 2019

Accepted for publication in *Information and Communications Technology Law* [https://www.tandfonline.com/loi/cict20]

Abstract: New approaches to the legal duties of Internet intermediaries are emerging. Current critiques of technology companies in what is said to be a 'techlash' overlaps with the proposing of new models of liability and responsibilities. Do these shifts in attitude, and the associated set of new ideas, mean that legislative bodies might be more willing, today, to revisit the balance struck in the late 1990s? Changes and challenges to the general provisions applicable to intermediaries, and the introduction of standalone provisions in specific sectors (such as audiovisual media regulation and copyright) are discussed; emphasis is placed on the proliferation of 'voluntary' measures (e.g. on illegal content and on disinformation), which provide evidence of changing attitudes. Further arguments include the overlap between available causes of action in relation to Internet communications (e.g. data protection and harassment law), with implications for jurisdiction, remedies, and other matters, and the attractiveness of alternative approaches, including the cross-cutting control of 'harmful digital communications' in New Zealand, and proposals to apply specific regulatory regimes, influenced by financial regulation and other fields, to online material. The UK government's recent ideas regarding a possible 'duty of care' for certain intermediaries assessed in the context of these developments.

Keywords: intermediary liability, copyright, audiovisual media services, social media, freedom of expression

1. Introduction

A generation ago, a first wave of Internet-related legislative changes and landmark cases in the late 1990s brought about a certain understanding of the regulation of content and, in particular, the role played by 'intermediaries'. Intermediaries, in this context, can include providers of Internet access ('ISPs' as often termed) and those who 'host' content created by others. Since then, the relevant technologies (and the ways in which they are used) have continued to develop; key changes include the growth in use of large social media platforms, advances in surveillance but also in encryption or obfuscation, and the gradual move towards always-on and mobile access through a broad range of devices. Are those turn-of-the-millennium laws accepted as the right framework for Internet content regulation today?

When new statutory provisions were first adopted regarding Internet intermediaries, the fundamental question was whether, and if so to what extent, to fix through legislation the degree of liability that would be faced by intermediaries, under existing

* Professor of law and innovation, Queen's University Belfast. d.macsithigh@qub.ac.uk. Based on work presented at the Cambridge Intellectual Property and Information Law Annual Conference (March 2018), Law Commission of Ontario conference 'Defamation Law in the Internet Age' (May 2018), Queen's University Belfast Judicial Forum (June 2018), and the NATO StratCom Centre of Excellence Expert Workshop 'Rule of law in the digital environment' (December 2018)

causes of action such as in defamation and other torts.[1] In the United States, the 1996 Communications Decency Act,[2] responding to conflicting doctrines emerging from defamation caselaw, broadly excluded the possibility of liability for all types of intermediary.[3] This applied not just to defamation but to private law actions in general, though with a notable exception for liability under intellectual property law. Specific federal copyright legislation of two years later, the Digital Millennium Copyright Act, established a more granular approach to liability – especially in stipulating conditional ('notice and takedown') rather than absolute immunity for hosts.[4] In the United Kingdom, the Defamation Act 1996 addressed in part the position of a category defined as those who were neither author, editor nor publisher of content.[5] Then, the 2000 Electronic Commerce Directive[6] (transposed through the Electronic Commerce Regulations 2002 in the UK, and referred to here as the ECD) established separate schemes governing the liability of mere conduits (ISPs), caches, and hosts; further provision was made in other areas of EU law, such as a clause on injunctions against third parties included in the 2001 Information Society Directive on copyright.[7]

Today, the role of the intermediary is under scrutiny in an especially intense way. Whether it be the evolving caselaw on liability,[8] or the consideration of statute-backed regulatory schemes, ensuring meaningful control over Internet content has (re)emerged as a controversial issue. With further legislative change seeming likely, the relatively terse statements of liability (or the lack thereof) of two decades ago, and narrower updates such as that which formed part of defamation reform in England and Wales more recently, no longer dominate academic analysis or political debate. Yet these more recent discussions are linked to a long-established assumption, which is that the legal exposure of intermediaries is a key (and often effective) lever through which the availability of Internet-delivered content to mainstream audiences can be controlled, even indirectly through the setting of incentives.

In 2013, I argued that the law on intermediaries was fragmenting, criticising not necessarily the concept of fragmentation itself (which could be justified in terms of harm, impact, or the like), but the lack of a clearly expressed normative basis for distinguishing between the obligations of service providers on the basis of the relevant body of law (e.g. copyright, defamation, or privacy).[9] Half a decade later, it is clear not just that fragmentation has continued, but that new approaches to the

---

[1] See e.g. Lilian Edwards, '"With Great Power Comes Great Responsibility?": The Rise of Platform Liability' in Lilian Edwards (ed), *Law, Policy and the Internet* (Hart 2018) 253-289.
[2] US Code, 47 USC 230.
[3] A full account of the CDA and its caselaw can be found in Eric Goldman, 'An Overview of the United States' Section 230 Internet Immunity' in Giancarlo Frosio (ed), *The Oxford Handbook of Intermediary Liability Online* (OUP 2019).
[4] Digital Millennium Copyright Act 1998; the intermediary provisions are found in US Code, 17 USC 512.
[5] s 1; this provision applied in England and Wales, Scotland, and Northern Ireland.
[6] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178, articles 12-15.
[7] Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167.
[8] Reviewed in commendable detail in Jaani Riordan, *The Liability of Internet Intermediaries* (OUP 2016).
[9] Daithí Mac Síthigh, 'The fragmentation of intermediary liability in the UK' (2013) 8 Journal of Intellectual Property Law and Practice 521.

whole question of regulating intermediaries are emerging. In particular, the present criticism of the power of technology companies - what some journalists have called a 'techlash', whereby the actions and responsibilities of powerful and successful technology companies are coming under greater scrutiny – is creating a space for new models of liability and duty to be proposed. Do these shifts in attitude, and the associated set of new ideas, mean that legislative bodies might be more willing, today, to revisit the balance struck in the late 1990s?

In part 2, I note various changes or challenges to the general provisions applicable to intermediaries, including the reviews carried out and recommendations made by the European Commission, and the interaction between legal provisions in specific sectors (such as audiovisual media regulation and copyright) and the general law on intermediary liability. Special emphasis is placed on the proliferation of (proposed and implemented) 'voluntary' measures (e.g. on illegal content and on disinformation), which provide evidence of changes in attitude albeit without (yet) leading to an amendment of the core provisions of the first wave.

In part 3, I proceed to make three observations regarding the present position, which I argue will shape the revisiting of the earlier settlement. The first point is the degree to which *attitudes* towards intermediaries have shifted; I find evidence for this in the statements of lawmakers and in human rights law. The second is the emerging impact of the *overlap* between available causes of action in relation to Internet communications (e.g. data protection and harassment law, not just defamation and privacy law), which affects intermediaries as well as the authors of the content itself, and has implications for jurisdiction, remedies, and other matters. The final point is the attractiveness of *alternative approaches*, including the cross-cutting control of 'harmful digital communications' in New Zealand, and proposals to apply specific regulatory regimes, influenced by financial regulation and other fields, to online material. In this section, the UK government's current thinking regarding a possible 'duty of care' for certain intermediaries is presented as part of and influenced by these broader developments.

2. New statutory and voluntary measures for intermediaries

2.1 The E-Commerce Directive (ECD) and beyond

It is first important to note that the apparent simplicity of the ECD does not tell the full story – if it ever did. Take for instance the position of a host, subject to the law of England and Wales, in respect of defamation law. Its liability is affected by a number of differently drafted defences and exclusions, stretching across domestic law (the 1996 Act, which applies across the UK), transposed EU law (the 2002 Regulations, read in light of the ECD and EU principles, of course), and the common law. Moreover, intermediary liability is also dealt with in the Defamation Act 2013 (albeit limited to England and Wales). The 2013 Act contains a further set of defences (ss 5 and 10), including a new scheme, supplemented by secondary legislation, for 'operators of a website'. The overlap between defences (even prior to the 2013 Act) complicates litigation.[10]

[10] See for instance *Tamiz v Google* (especially at first instance: [2012] EWHC 449 (QB), [2014] EMLR 24); see further the alternative approach in *Metropolitan International Schools v Designtechnica* [2009] EWHC 1765 (QB), [2010] 3 All ER 548 (although statutory defences were unavailable, the claim failed as Google's functions in operating a search engine did not constitute publication).

More generally, certain ambiguities in the ECD, including its relationship with other legislation, have been teased out through preliminary references to the CJEU. Injunctions against service providers (conduits and hosts) are possible, though must be proportionate.[11] Hosting includes social networking sites[12] and encompasses ad-supported 'free' services as well as paid services[13], but not content created by the host itself,[14] or activity that is not of a 'merely technical, automatic and passive nature.'[15] In parallel, the European Commission has kept the ECD under review. Its 2012 assessment[16] identified four areas of particular uncertainty in the law: definitions (e.g. what constitutes hosting), conditions required for protection, the operation of notice and takedown, and the extent to which monitoring is possible or required. This was followed by a consultation and related activity, though no legislative change.

2.2 From liability towards duty

Evidence of a 'techlash' is likely to be found in the first instance in a hardening of language rather than a fully-formed proposal for revising the law. For instance, the European Commission, in a 2017 Communication on Illegal Content, argues that '(t)he open digital spaces [online platforms] provide must not become breeding grounds for … spaces that escape the rule of law'.[17] In the UK, a parliamentary committee recommended that 'a new category of tech company [be] formulated, which tightens tech companies' liabilities, and which is not necessarily either a 'platform' or a 'publisher'"[18]

Statements of this nature are consistent with a shift that others have observed, whereby a 'media' model of liability is being discussed more frequently, despite the 'telecoms' origins of liability rules.[19] The ECD provided a telecoms-style broad shield to mere conduits, with stronger (but still far from 'media') obligations for hosts. These provisions, and their persistence over two decades, embedded in political and legal discourses an assumption that an exemption of liability is 'not only necessary but also sufficient to safeguard the free flow of information and users' freedom'.[20] Now, the refocusing of legislative and political effort on obligations and duties even in

---

[11] Case C-70/10 *SABAM v Scarlet* [2011] ECR I-11959; Case C-314/12 *UPC Telekabel Wien v Constantin Film* [2014] Bus LR 541; Case C-484/14 *McFadden v Sony* [2017] Bus LR 430 (also considering costs).

[12] Case C-360/10 *SABAM v Netlog* [2012] 2 CMLR 18; see a more extensive list of the services that have been found to fall within the scope of article 14 ECD in David Erdos, 'Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU acquis' (2018) 26 International Journal of Law and Information Technology 189, 195-8.

[13] Case C-291/13 *Papasavvas* [2015] 1 CMLR 24.

[14] Ibid.

[15] Case C-324/09 *L'Oreal v eBay* [2012] EMLR 6; Case C-236/08 *Google France v Louis Vuitton* [2010] ECR I-2417.

[16] European Commission, 'A coherent framework for building trust in the digital single market for e-commerce and online services' COM(2011) 942.

[17] European Commission, 'Tacking Illegal Content Online' COM(2017) 555.

[18] House of Commons Digital Culture Media and Sport Committee, *Disinformation and 'fake news': Interim Report* (HC 363, 2017-19) [58]; House of Commons Digital Culture Media and Sport Committee, *Disinformation and 'fake news': Final Report* (HC 1791, 2017-19) [13-14].

[19] See e.g. 'Internet firms face a global techlash' *The Economist* (10 August 2017).

[20] Niva Elkin-Koren, 'After twenty years: revisiting copyright liability of online intermediaries' in Susy Frankel and Daniel Gervais (eds), *The evolution and equilibrium of copyright in the digital age* (Cambridge University Press 2014) 30.

situations where a service provider does not carry liability acknowledges the limitations of the dichotomy.

We can see the gradual development of new attitudes to intermediaries in the work of the European Commission, especially within its Digital Single Market agenda. The question of liability is specifically noted as one of the areas where the Commission sees a role for the reform of law and policy in order to provide for the better regulation of an emerging category of 'platforms'. The Commission also emphasises, in its broader work on how platforms 'increasingly (take) centre stage … in respect of access to information and content',[21] the 'wider responsibility' associated with these functions. The reframing of intermediaries as platforms[22] serves in particular to recall the degree to which there is little common ground on the power of intermediaries to regulate: as Lynskey puts it, platforms are gatekeepers, which 'control what content we access and the terms on which this content can be accessed', while individuals 'lack the knowledge and power to have a disciplining influence' due to the lack of knowledge of how this control is exercised.[23]

In a mid-term review of the Digital Single Market initiative, the Commission committed to providing 'guidance on liability rules and support to platforms on voluntary measures taken by platforms when they work proactively to remove illegal content, acting in good faith' and coordinating effective, transparent and proportionate technical solutions for removal.[24] A 'balanced and predictable liability regime' should be maintained, it argued, but in a context where a 'sustainable approach' will require the further consideration of illegal and harmful material.[25]

Changing attitudes are also found in discrete areas of law, where the extant provisions on intermediaries are not explicitly being reviewed, but are challenged by the creation of new duties or regulatory requirements. In the following sections, three such legislative changes – all of which have been adopted over a two-year period – are considered. The first two are clearly drawn from a media regulation tradition (blocking requirements, and the emerging category of 'video-sharing platforms', while the third (copyright) sees a further new model of a role for intermediaries.[26]

2.3 Statutory measures in specific areas

2.3.1 Blocking

---

[21] European Commission, 'Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe' COM(2016) 288 ['Platforms Communication'].

[22] Not just by the European Commission; see e.g. House of Lords EU Select Committee, 'Online Platforms and the Digital Single Market' (HL 2015-16, 129).

[23] Orla Lynskey, 'Regulating 'platform power'' LSE Law, Society and Economy Working Papers 1/2017 <https://dx.doi.org/10.2139/ssrn.2921021> .

[24] European Commission, 'Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All' COM(2017) 228, p 9.

[25] Platforms Communication (n 21) 8.

[26] Other areas of law could also have been chosen for analysis, but the three highlighted here have recently reached the end of the statutory revision process and so offer the most complete text. For instance, recent (and as yet unimplemented) reviews of contempt law have considered the merits of a clearer statutory power to order the temporary removal of material published before proceedings became active, with some debate on the extent to which this would be expressed against hosts and other intermediaries: Law Commission, *Contempt of Court: Juror Misconduct and Internet Publications* (Law Com No 340, 2013); New Zealand Law Commission, *Contempt in Modern New Zealand* (NZLC IP36, 2014) [4.71] and [4.77]; see further D Mac Síthigh, 'Contempt of court and new media' in Gillies & Mangan (eds), *The legal challenges of social media* (Edward Elgar 2017).

The primary type of new requirement for intermediaries under UK law has been obligations to 'block' access to content. The idea that Internet service providers (mere conduits in ECD terms) would block access by users to specified websites or pages was first found in the UK on a non-statutory basis in respect of indecent images of children.[27] Subsequently, numerous court orders in respect of intellectual property infringements have required blocking of named URLs by the respondent ISPs; the legal basis has been s 97A Copyright, Designs and Patents Act 1988 (inserted 2003 in transposition of article 8(3) of the Information Society Directive) in respect of copyright, and s 37(1) Senior Courts Act 1981[28], read in light of an untransposed clause in the IP Rights Enforcement Directive[29], in respect of trademarks.[30]

A third model is distinctive through being a detailed regulatory scheme, found in primary legislation and supporting statutory instruments. This is the new requirement for ISPs to block access to websites not compliant with the new UK rules on age verification for sites containing sexually explicit material, set out in Digital Economy Act 2017. The new age verification regulator (which will be the existing cinema and video classification body, the BBFC) will exercise functions in relation to (a) content providers, (b) payment-services providers, (c) ancillary service providers e.g. advertisers, and (d) Internet service providers. While the functions for (b) and (c) are that they are only notified of the non-compliance of their clients, ISPs will be required to block.[31]

The prohibition of publishing the relevant material without age verification goes beyond the requirements of EU law, both in terms of *scope* (with the EU-mandated provision confined to services that meet the various aspects of the definition of an on-demand audiovisual media service, including that the service be 'TV-like'; the new UK provision also includes audio material and still images) and *effect* (applying to pornographic content including that equivalent to video works rated 18 by the BBFC, rather than the narrower class of content that member states are obliged to control under the AVMS Directive, discussed in 2.3.2 below). It is however confined to material distributed on a commercial basis (the details of which are set out in the secondary legislation).

2.3.2 Video-sharing platforms

---

[27] For detailed accounts of this system, and the role of the body responsible for it (Internet Watch Foundation), see TJ McIntyre, 'Internet Censorship in the United Kingdom: National Schemes and European Norms' in Lilian Edwards (ed), *Law, Policy and the Internet* (Hart 2018) 291-330; Christopher Marsden, *Internet co-regulation : European law, regulatory governance and legitimacy in cyberspace* (Cambridge University Press 2011) 168-195; Emily B. Laidlaw, *Regulating speech in cyberspace : gatekeepers, human rights and corporate responsibility* (Cambridge University Press 2015) 123-169.

[28] Note also a use of the equitable powers of the court (absent any more detailed statutory provisions) in an industrial IP case in British Columbia to require Google to delist an IP-infringing website: *Google v Equustek* 2017 SCC 34, applying Law and Equity Act, RSBC 1996, ch 253, s 39.

[29] Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L157/16, article 11. (In Northern Ireland, see Judicature (Northern Ireland) Act 1978, s 91; in Scotland, see Court of Session Act 1988, s 47(2)).

[30] *Cartier v British Sky Broadcasting* [2016] EWCA Civ 658, [2017] 1 All ER 700 (principle); [2018] UKSC 28, [2018] 4 All ER 373 (costs).

[31] Digital Economy Act 2017, s 14 (content providers), s 21 (payment and ancillary services), s 23 (ISPs).

Media regulation, which since 2007 includes EU provisions on on-demand audiovisual media services, is also becoming more relevant for intermediaries. EU law now includes a new category of video sharing platforms, adopted in a 2018 amendment to the Audiovisual Media Services Directive (AVMSD) and currently being transposed by member states.[32] The new requirements applies to services with a principal purpose of 'providing programmes and user-generated videos to the general public, in order to inform, entertain or educate'.

Until 2018, it has been the case that video sharing platforms were unlikely to fall within the AVMSD, as even its 'on-demand audiovisual media service' category, added in 2007, was predicated upon the service provider having 'editorial responsibility' for the content (and meeting other tests). Such services had, until 2007, fallen within the ECD alone, and were therefore, in common with online content in general, not subject to specific rules on content under EU law.[33] The 2007 changes brought certain non-linear services (including popular services subsequently launched in Europe, such as Netflix) within the AVMS rules. On the other hand, a service like YouTube was not deemed to fit the definition - although a content provider uploading material to YouTube might, subject to various other tests. As such, the VSP category added in 2018 is explicitly addressed to services that do *not* exercise editorial responsibility; member states are now obliged to ensure that providers take 'appropriate measures' against hate speech and to protect children, such as age verification, parental controls, and the use of terms and conditions.

These requirements are mitigated by a number of further definitions. Adding possible breadth to the rule, the principal purpose requirement can be applied to a service or to a dissociable section thereof, addressing an issue under the 2007 rules where mixed services (e.g. a newspaper's website containing video) could be found to have a principal purpose other than the supply of video and so fall outside the scope of the AVMSD.[34] On the other hand, the scope is narrowed by how services are defined. The Commission's first version was restricted to services consisting of the 'storage of a large amount of programmes or user-generated videos',[35] but the Council proposed instead referring to the 'storage of programmes or user-generated videos' (that is, without the reference to a 'large amount').[36] The final result was a more general reference to providing programmes or user-generated videos, with a proviso

---

[32] Directive 2018/1808 of 14 November 2018 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. References to the AVMSD in this article are therefore to the 2010 Directive (which was a consolidation of the Directives of 1989, 1997 and 2007) as amended by Directive 2018/1808. An unofficial consolidation is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805240/_Annex_D__Unofficial_consolidation_showing_amendments_made_by_the_2018_AVMS_Directive__2018_1808_EU__to_the_2010_AVMS_Directive__2010_13_EU_.pdf.

[33] Rachael Craufurd Smith, 'Media convergence and the regulation of audiovisual content' (2007) 70 Curent Legal Problems 238; Daithí Mac Síthigh, 'Co-regulation, video-on-demand and the legal status of audio-visual media' (2011) 2 International Journal of Digital Televison 49, 53-5.

[34] Irini Katsirea, 'Electronic press: 'Press-like' or 'television-like'?' (2015) 23 International Journal of Law and Information Technology 134; Lorna Woods, 'Video-sharing platforms in the revised Audiovisual Media Services Directive' (2018) 23 Communications Law 127, 130; Case C-347/14 *New Media Online GmbH* v *Bundeskommunikationssenat* [2016] 2 CMLR 14.

[35] COM(2016) 287, draft article 1(1)(aa).

[36] Council of the European Union, document 9691/17 (24 May 2017), draft article 1(1)(aa).

that the required measures '(take) into account the size of the video-sharing platform service and the nature of the service that is provided'.[37]

Although this new category is explicitly *not* predicated on editorial responsibility, it does only apply where the organisation of the content is 'determined by the provider of the service' including by an algorithm or automatic means.[38] In practice, this means that sites consisting of user-uploaded video will be subject to the new requirements, as could social networking sites (if they meet the above-noted tests). However, along with the new category comes a particular set of requirements – narrower than either the first or second category under the 2007 AVMSD, but arguably more interventionist than currently required under the general provisions of the ECD.

The obligation is upon member states to 'ensure that video-sharing platform providers take appropriate measures' on the grounds of the protection of minors (against content 'which may impair their physical, mental or moral development', the protection of citizens against content 'containing incitement to violence or hatred', and – added later in the legislative process – 'provocation to commit a terrorist offence'.[39] The first two of these three categories (minors and hate), though with stronger regulatory requirements, are already found in the AVMSD in respect of TV and on-demand services, while the third is justified by reference to the new provisions of the Terrorism Directive.[40]

The AVMSD further provides a list of 'practicable and proportionate' appropriate measures, including the regulation of such content through terms and conditions, systems for user reporting, flagging and rating, and (for content harmful to minors) age verification and parental controls.[41] The Parliament had proposed that 'any ex-ante control measures or upload-filtering of content' be prohibited; a weaker version of this text (prohibiting only ex ante measures which do not comply with the existing terms of article 15 ECD) was included, alongside further language around the right of users to assert rights and turn to legal proceedings where they disagree with, for instance, a decision to remove a video uploaded by that user.[42]

Of course, as hinted above, the requirements for video-sharing platforms will be less onerous than the existing AVMSD; e.g. member states must *ensure* that TV and on-demand services 'do not contain' hate content and are 'only made available in such a way as to ensure that minors will not normally hear or see' the content which may impair their development.[43] On the other hand, although quite familiar for regulated providers of television and on-demand services, they represent a new legal duty (perhaps mapping onto existing voluntary action in some but not all cases[44]) for

[37] AVMSD (n 32), art 1(1)(aa) and art 28b(3).
[38] Ibid, art 1(1)(aa).
[39] Ibid, art 28b(1).
[40] Directive (EU) 2017/541 of 15 March 2017 on combating terrorism.
[41] AVMSD (n 32) art 28b(3).
[42] European Parliament, document A8-0192/2017 (10 May 2017).
[43] AVMSD (n 32) art 6(1)(a) and art 6a(1).
[44] The UK, which opposed the proposal in principle and voted against it, noted nonetheless that 'many of the requirements are already captured in the terms and conditions of existing social media platforms.'

those who operate the subset of intermediaries that meet the video-sharing platform definition.

There was also a telling debate as to the nature of harmonisation in this field. The Commission' had proposed that member states be prohibited from applying further requirements to video-sharing platforms, except in respect of illegal content.[45] This is consistent with the general restriction on specific regulation by the law of a member state under the original ECD, and of course the proposals here make direct reference to additional regulation being in accordance with EU law (including the ECD). Nonetheless, the majority in the Council wished to go further, and make the clause one of minimum harmonisation only (that is, member states would be free to impose stricter requirements, whether in respect of illegal content or otherwise).[46] The Council's view was preferred, and it is explicitly permitted for member states to go further[47] (subject to existing rules of EU law; the intermediary liability provisions of the ECD are mentioned as an example, as are the provisions and safeguards on blocking of images of child sexual abuse[48]).

2.3.3 Copyright

As compared with other areas of the regulation of Internet intermediaries (and online activity more generally), copyright has seen consistent legislative attention – and a high number of preliminary references to the CJEU – in the 21st century.[49] New and controversial obligations for another subset of intermediaries were the most-debated aspect of a new copyright Directive adopted in 2019. This very recent revision of copyright law provides important evidence of the issues that arise when it is proposed that new obligations be imposed upon intermediaries, even if only having an immediate impact on certain providers and in respect of certain types of exposure to liability.

New Directive 2019/790[50] amends or builds upon various provisions of the 2001 Information Society Directive. New obligations are created, in article 17[51] for (for-profit) service providers that 'store and give the public access to a large amount of copyright-protected works or other protected subject matter' uploaded by users. This is justified in a Recital by reference to the complex online market, where services containing infringing material 'have become a main source of access to content online'.[52] There are exceptions, including for 'not-for-profit online encyclopaedias' (art 2(6)), and the imposition of a more limited set of obligations for smaller start-up

[45] COM(2016) 287, draft article 28a(5).
[46] Document 9691/17 (n 36), draft article 28a(5).
[47] AVSMD (n 32) art 28b(6).
[48] Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography [2011] OJ L355/1, art 25.
[49] A thorough account of the caselaw under the 2001 Information Society Directive, emphasising the growth in significance of injunctions, is found in Martin Husovec, *Injunctions Against Intermediaries in the European Union: accountable but not liable?* (Cambridge University Press 2017)
[50] Directive 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, [2019] OJ L130/92.
[51] Numbered as article 13 in its draft version (and so familiar to many readers in that numbering from the energetic campaigns for and against its adoption); see e.g. Felipe Romero-Moreno, ''Notice and staydown' and social media: amending Article 13 of the Proposed Directive on Copyright' (2019) 33 International Review of Law, Computers & Technology 187.
[52] Directive 2019/790 (n 50), recital 37.

service providers (art 17(6)) – subject to an early review of the effectiveness of differential treatment (art 30(1)).

What is now required of the subset of intermediaries now caught by the 2019 Directive? Essentially there are three possible situations. Firstly, a service provider can reach an agreement with rightsholders, and so be 'authorised' in respect of its activities (art 17(2)). Secondly, where there is no authorisation in place, it can follow the instructions of the 2019 Directive (make best efforts to obtain an authorisation, make best efforts to limit the availability of protected works, and follow a modified version of notice and takedown including a 'staydown' provision) (art 17(4)). Lastly, it can do neither, but can then be found liable for unauthorised communication to the public. 'Stakeholder dialogues' to work out matters such as best practices for professional diligence in respect of the matters covered by article 17 are to be organised.

In new article 17 and recital 64, it is argued that storing and providing access constitutes communication or making available to the public under copyright law, and that article 14 ECD does not limit this liability. It had been noted, at proposal stage, that qualification for ECD protection requires consideration of whether the service provider plays an active role, including promoting or optimising the presentation of material. This was clearly a deliberate reference to the limitations to article 14, albeit placed in the context of a copyright-specific piece of legislation. If true, the implications are broader than copyright law. However, the point is not confronted in the final version of article 17, with blunter approach of stripping affected service providers of article 14 protection (in respect of the activities within its scope) having been taken. The result is to create a new approach to duties and liability, confined to a subset of intermediaries and to copyright law alone, but markedly different in tone and scope to the ECD. The political controversy surrounding its adoption is reflected in the length of individual Recitals (recital 66, for instance, runs to close to a thousand words) and in the various belt-and-braces references to proportionality, balance, and the avoidance of general monitoring obligations.

2.4 'Voluntary' measures

Alongside the legislative measures in media and copyright law, as discussed above, the last three years has also seen ongoing European Commission activity regarding 'voluntary measures', which have been increasingly expressed in firmer terms - though not, as yet, forming a proposal for new legal obligations. The key activity is found across four successive instruments: a 2016 Code of Conduct on hate speech,[53] a 2017 Communication on Illegal Content,[54] a 2018 Recommendation on Illegal Content,[55] and finally a 2018 Communication on 'disinformation'.[56]

The *Code of Conduct* has the narrowest focus, upon 'hate speech'. It calls for the expeditious review of valid notifications by 'online intermediaries and social media

[53] European Commission, 'Code of Conduct on countering illegal hate speech online' (30 June 2016) https://ec.europa.eu/newsroom/just/document.cfm?doc_id=42985.
[54] COM(2017) 555 (n 17).
[55] Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, C(2018) 1177 ['Illegal Content Recommendation'].
[56] European Commission, 'Tackling online disinformation: a European approach', COM(2018) 236 ['Disinformation Communication']

platforms', with a target of 24 hours set out in an accompanying press release.[57] The 2017 *Communication* emphasises the responsibilities of service providers for a broader class of 'illegal content' (defined as content that is illegal). The most ambitious recommendation is for 'effective proactive measures to detect and remove' such content. This can be brought about through the use of trusted flaggers (and making user flagging easier) and the application of rights-compliant criteria. Various safeguards ('to limit the risk of removal of legal content') are called for, i.e. transparency and accountability, including something akin to the counter-notice system familiar in respect of US copyright law (though not a requirement of existing EU law on intermediaries under the ECD).

Subsequently, the Commission issued a *Recommendation* (March 2018), framed as 'safeguard(ing) the balanced approach that [the ECD] seeks to ensure'. Much of the Recommendation, including the general concept of illegal content, is carried forward from the Communication. 'Proportionate and specific proactive measures' to restrict illegal content in general are encouraged, though with caution around the use of automation (article 18). For a subcategory of 'terrorist' content, the caution around automation is explicitly disavowed, and a target of removal on the basis of notice within an hour is added. Member states are encouraged to establish new reporting obligations for service providers. Counter notice systems are recommended, except in the case of serious criminal offences involving threat to life / safety of persons (articles 9/11); further provisions encourage transparency and protection against bad faith use of notice mechanisms (articles 16/21). Neither the Communication nor the Recommendation are confined to the narrower category of material that is illegal to access/download, and so appear to include material the communication or publication of which violates the law.

The approach taken in both instruments prompts an immediate question as to whether voluntary activity on the part of a host would deprive it of its protection against liability. The 2017 Communication includes a discussion of the *L'Oréal* limitation to protection (where the service provider plays an active role[58]), and goes on to admit that loss of exemption through becoming aware of facts and circumstances is possible. However, it does not characterise this as a problem, as having become aware, the host can then take action (i.e. remove the content) so as to continue to avoid liability. As such, article 14 should not 'deter or preclude' compliance with the new (advised) measures. The 2018 Recommendation does no more than refer back to the reasoning in the 2017 Communication (recital 26).This reference to *L'Oréal*, which also arose during the debate on revising the Information Society (Copyright) Directive, is clearly intended to signal (within the context of the subject matter of each instrument, though clearly equally applicable in other fields covered by the ECD) that there are limits to the applicability of article 14. Indeed, the implications of *L'Oréal* are not yet fully explored. The point is considered *obiter* in the English copyright case of *Tixdaq*, where Arnold J expresses a provisional view that article 14 does not protect service providers where 'editorial review' of material uploaded by users has taken place.[59] In Northern Irish cases, the complexity of awareness has been noted; in *CG*, this was colourfully expressed as Facebook not

[57] European Commission, 'European Commission and IT Companies announce Code of Conduct on illegal online hate speech' (press release, 31 May 2016) http://europa.eu/rapid/press-release_IP-16-1937_en.htm.
[58] *L'Oréal v eBay* (n 15) [113] and [116].
[59] *England And Wales Cricket Board v Tixdaq* [2016] EWHC 575 (Ch), [2017] ECDR 2 [170]

being ‘entitled to close their eyes’ to the breach of privacy contained on a page about which they had been made aware through correspondence,[60] while in *JR20*, the problems associated with Facebook’s online system for reporting violations of its ‘Community Standards’ were considered at first instance and noted on appeal.[61]

Alongside its interest in illegal content, the Commission has also developed a body of work regarding ‘disinformation’, addressing many of the issues often debated under the ill-fitting ‘fake news’ label. This work, encapsulated in an April 2018 Communication,[62] cross-references other developments, including the new video-sharing platform category, the Communication and Recommendation on illegal content, copyright, and data protection.[63] However, the key justification is the protection of the fairness of elections, with the ‘viral’ dimension highlighted as a complicating factor. The Commission is, for now, proceeding through a code of conduct[64] (signed in September 2018 by Facebook, Google, Twitter, Mozilla and – in 2019 - Microsoft), with regular monitoring reports highlighting the (voluntary) actions being taken by service providers. The strategic significance of the code of conduct can be seen in, for instance, reference to it (and to details of how compliance is being monitored) in a December 2018 action plan on disinformation, jointly produced by the Commission and the EU’s high representative for foreign affairs and security policy.[65]

3. Beyond liability

3.1 New approaches

Both the statutory measures and voluntary measures discussed in part 2 share a set of assumptions regarding the role that intermediaries can play in addressing pressing problems relating to Internet communications. These arguments often turn on the moral responsibilities of such companies, alongside a presumption that the nature of the functions they perform, and their relationship with users, makes their actions more effective (or at least more timely) than alternatives.

In this part, I explore these assumptions in more detail, showing that the changes introduced in part 2, alongside measures in other jurisdictions or now proposed for consideration in the United Kingdom, reflect a new, responsibility-based model of intermediary action that seeks to preserve on the statute book existing protections against liability for intermediaries while in fact fixing them with significant new obligations.

3.2 Attitudes

A decade ago, the rhetorical device of pointing to the specific roles that ought to follow from with (moral) responsibilities was particularly prevalent in debates on intellectual property – especially as the efforts of rightsholders moved away from a blunt strategy of legal action (including towards end users) towards reducing access

[60] *CG v Facebook Ireland* [2016] NICA 54, [2017] EMLR 12 [72].
[61] *JR20 v Facebook Ireland* [2016] NIQB 98 [74]; [2017] NICA 48 [41].
[62] Disinformation Communication (n 56).
[63] Ibid.
[64] European Commission, ‘EU Code of practice on disinformation’ (September 2018) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.
[65] ‘Action plan against disinformation’ JOIN(2018) 36.

to infringing material with the assistance or action of intermediaries. As music manager Paul McGuinness put it in a 2008 speech at Cannes, the financial position of the industry ('as the companies react to falling revenues by cutting staff') should 'shame' service providers into starting to take 'responsibility for the content they've profited from'.[66] Nearly a decade later, similar arguments are found in the Home Secretary's speech to the Conservative Party conference in October 2017 included a call on service providers to 'honour (their) moral obligations' through devising and implementing technological solutions for the removal of terrorist material.[67] In the broader context of hate speech, this argument is made particularly bluntly by the Home Affairs Select Committee:

> The major social media companies are big enough, rich enough and clever enough to sort this problem out—as they have proved they can do in relation to advertising or copyright. It is shameful that they have failed to use the same ingenuity to protect public safety and abide by the law as they have to protect their own income.[68]

This view is not universally held. In addressing an ambiguity (regarding costs) in the existing legislative requirements in respect of third parties under intellectual property law (the IPRED provisions discussed at 2.2, above), the Supreme Court was sceptical regarding the relevance of the 'moral' dimension (per Lord Sumption):

> It has sometimes been suggested that because ISPs benefit financially from the volume and appeal of the content available on the internet, including content which infringes intellectual property rights, it is fair to make them contribute to the cost of enforcement The difficulty that I have with it as a matter of English law is that it assumes a degree of responsibility on the part of the intermediary which does not correspond to any legal standard. The suggestion appears to be that there is a moral or commercial responsibility in the absence of a legal one. But the law is not generally concerned with moral or commercial responsibilities except as an arguable basis for legal ones.[69]

Nonetheless, references to the bringing across of solutions developed in one (*legal*) context to a broader set of obligations has continued to form an important aspect of *political* discussions regarding intermediaries. An obvious example is the emphasis placed on the smooth running of the (non-statutory) system for blocking URLs pointing to (illegal) indecent images of children through the Internet Watch Foundation's list and the various technologies used by ISPs to implement it, in the subsequent cases on the (statutory, albeit arguably less morally clear cut) blocking of IP-infringing websites (see 2.3.1, above).

Alongside these developments, a familiar debate on whether obligations placed upon intermediaries actually acts against the common good, through promoting unaccountable private censorship,[70] re-emerges. Note, for instance, the developing interest of the European Court of Human Rights in the question of intermediary

---

[66] Speech at MIDEM Cannes, 28 January 2008, reprinted in *Sunday Times* (16 March 2008).
[67] Amber Rudd, speech at the Conservative party conference, 3 October 2017 https://www.bbc.co.uk/programmes/b09b2g0m.
[68] Home Affairs Select Committee, *Hate crime: abuse, hate and extremism online* (HC 2016-17, 69) [36]
[69] *Cartier* (n 30) [34].
[70] See e.g. Laidlaw (n 27).

liability. In *Delfi*,[71] the liability of an Estonian news website for comments posted on it was found not to violate the freedom of expression guaranteed in article 10; the case was distinctive for how the concurring and dissenting opinions saw very different visions of Internet communication – Judge Zupančič, concurring, offering strong criticism of the abusive and unsubstantiated nature of some online material, matched by Judges Sajó and Tsotsoria, in dissent, contending that the imposition of liability was a threat to free speech and to the proper functioning of the Internet itself. The majority, however, worked on a more limited basis and was content that obligations on a news portal as in the service in question could not be equated to private censorship.[72] Subsequently, in *Magyar Jeti*, Judge Pinto de Alberquerque's concurring opinion explored the importance of hyperlinks to the good functioning of the Internet, with repeated references to the work of Web founder Tim Berners-Lee. This echoes another theme in the *Delfi* dissent, where emphasis was placed on the risks of collateral censorship and the history of the control of expression through the regulation of printers.[73]

New EU provisions on video-sharing platforms (see 2.3.3, above) represent a discursive shift towards a 'media' paradigm, for services that have fallen squarely within the general category of information society services under the ECD for the last two decades. Non-legislative measures, such as the 'illegal content' documents issued in recent years by the European Commission (see 2.4, above), point towards special responsibilities for platforms who do not exercise editorial control in a conventional sense. But hints are also found in *Delfi*: 'because of the particular nature of the Internet, the "duties and responsibilities" that are to be conferred on an Internet news portal for the purposes of Article 10 may differ to some degree from those of a traditional publisher, as regards third-party content'.[74] This paragraph is then cited in the December 2018 decision in *Magyar Jeti*, albeit in a context where the court is drawing a limit to responsibility in the narrower case of linking. Cumulatively, though, what seems to emerge is a new notion of responsibility, though still not 'editorial responsibility' in a full sense; this parallels Husovec's accountability/liability distinction in respect of intermediaries and copyright law.[75]

3.3 Complexity

3.3.1 Multiple causes of action

The options available to private law applicants in cases concerning online material should be noted, disclosing as it does the overlapping relevance of various causes of action and so the evolution in the nature of liability that intermediaries may face. In England and Wales, the High Court now defines media and communications law (for listing and hearing purposes) as claims in defamation, misuse of private information, data protection law, harassment by publication, and (optionally) other actions involving publication or other media activities.[76] In practice, an applicant wishing to

[71] *Delfi AS v Estonia* (2016) 62 EHRR 6.
[72] Ibid.
[73] See also Ronan Ó Fathaigh, 'The chilling effect of liability for online reader comments' [2017] European Human Rights Law Review 387, arguing that later decisions, such as *Pihl v Sweden* App no 74742/14 (ECtHR, 9 March 2017), offer a more extensive engagement with the human rights problems associated with intermediary liability.
[74] *Delfi* (n 71) [113].
[75] Husovec (n 49).
[76] Initiated in 2017 as a 'media and communications' list within the High Court, though with no statutory or rule basis (see *Mezvinsky v Associated Newspapers* [2018] EWHC 1261 (Ch), [2018]

ensure that problematic material is removed may make a case using two (or more) of these actions, driven by a desire to see the material removed or made less readily available to the public. A new pre-action protocol for media and communications, replacing a defamation-only predecessor, is intended to operate across causes of action.

A recent cluster of cases in Northern Ireland provide good evidence of this emerging practice and its implications for intermediaries; in *CG*,[77] the action encompassed misuse of private information, data protection harassment, and (albeit quickly abandoned) defamation, while *JR20*[78] included harassment and misuse of private information, *AY*[79] included data protection, misuse of private information, negligence, and harassment, and *Townsend v Google*[80] included breach of confidence (abandoned early), misuse of private information, and data protection. For present purposes, the implications of this phenomenon are threefold; the defences available to available to intermediaries will vary in relation to a single aggrieved party, different remedies may be available, and a service provider may be within the scope of one law (in terms of jurisdiction) but outwith another.

3.3.2 Defences

Turning first to *defences*, we can note an enduring lack of clarity regarding the relationship between the Data Protection Directive and the liability provisions of the ECD, as acknowledged in *CG*.[81] The new General Data Protection Regulation notes that it 'shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive',[82] though what this means in practice is still being debated.[83] A second example is found in respect of privacy actions in England and Wales, which are unaffected by the 2013 defamation law reforms, meaning that the new (defendant-friendly) statutory provisions in respect of the operators of websites have no relevance for privacy actions against such operators (who would continue to rely on the ECD alone, where applicable).

These differences in defences also affect the assessment of more general questions such as the protection of fundamental rights. In the ECtHR's decision in *Pihl*,[84] it was noted that even where a host has no obligation to remove content, an applicant is nonetheless able to rely upon data protection law to seek the deindexing of the material (or what the court less accurately calls requesting 'that the search engines remove any such traces of the comment'). As this was a case where it was argued that the exclusion from liability denied a remedy to a wronged party (i.e. a violation of article 13 ECHR), the *availability* of a remedy under data protection law is used to

FSR 28 [13]); see now CPR Pt 53, in effect from 1 October 2019, governing the now 'specialist list' for media and communications. The definitions are found in rule 53.1, with the pre-action protocol in Practice Direction 53B.

[77] *CG* (n 60).

[78] *JR20* (n 60).

[79] [2016] NIQB 76.

[80] [2017] NIQB 81.

[81] *CG* (n 60) [95].

[82] Regulation 2016/679/EU 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, [2016] OJ L119/1 ['GDPR'], art 2(3).

[83] Erdos (n 12) 194-5.

[84] *Pihl* (n 73) [33].

justify the *absence* of a remedy in defamation law (where the more general rules applied). Similarly, the emergence of 'right to be forgotten' arguments (under the 1995 Data Protection Directive and relying in part on the decision in *Google Spain*[85]) against search engine operators in domestic law – in *Townsend*[86] in Northern Ireland and the more recent English decisions in *NT1* and *NT2*[87] - demonstrates the more complex set of duties with which some intermediaries are being fixed in their capacity as data controllers, potentially without a general defence to liability.[88] This is further emphasised by the coming into force of the GDPR, with its clearer textual basis for a 'right to erasure' in its article 17, again framed as a freestanding obligation rather than related to liability.

3.3.3 Remedies

Secondly, the *remedies* available will be linked to the cause of action. Recent reforms to defamation law have included some changes to remedies. The Defamation Act 2009 in Ireland made provision for correction orders (s 30), while the 2013 Act in England and Wales include ordering the publishing of a summary of a court's decision (s 12). This 'counterspeech' approach could address some aspects of online communications, though for the time being is only available in defamation proceedings. In mainstream broadcasting law, a 'right of reply' concept is well recognised (although constitutionally problematic in the US[89]). It forms part of EU media law, and is implemented in various ways - e.g. through the Broadcasting Code in the UK but through standalone legislation in the Republic of Ireland.[90] However, the right of reply is only available in respect of television services, and not on-demand services or video-sharing platform services.[91] Meanwhile, caselaw has confirmed the availability of damages in data protection proceedings, especially for deliberate breaches and for subsequent harm resulting from unlawfully processed data, and including distress as well as financial loss.[92]

3.3.4 Jurisdiction

Finally, analysis of the measures discussed in part 2 above discloses a potential issue regarding the ever-present question of *jurisdiction*, which has long, in light of the transnational operations and varying corporate structures of key platforms, been an issue in the application of legal measures to Internet communications. Famously, early (and much-discussed) cases addressed the threshold question of jurisdiction in Internet defamation cases (e.g. *Dow Jones v Gutnick*[93] in the High Court of

---

[85] Case C-131/12 *Google Spain v AEPD* [2014] 3 CMLR 50.
[86] n 80.
[87] [2018] EWHC 799 (QB), [2019] QB 344.
[88] Erdos (n 12) 199 (noting also that Google did not rely on an ECD shield in *NT1*).
[89] *Miami Herald v Tornillo* 418 US 241 (1974).
[90] Broadcasting Act 2009, s 49.
[91] AVMSD (n 32) art 28.
[92] On the Data Protection Directive, and English law, see *Halliday v Creation Consumer Finance* [2013] EWCA Civ 333; *Vidal-Hall v Google* [2015] EWCA Civ 311, [2016] QB 1003; *TLT v Home Secretary* [2016] EWHC 2217 (QB). On the GDPR, see Eoin O'Dell, 'Compensation for Breach of the General Data Protection Regulation' (2017) 40 Dublin University Law Journal 97.
[93] [2002] HCA 56. There is an extensive literature on the decision and its impact; see e.g. David Rolph, 'Publication, innocent dissemination and the Internet after *Dow Jones & Co v Gutnick*' (2010) 33 University of NSW Law Journal 562; Alan Trammell and Derek Bambauer, 'Personal jurisdiction and the 'interwebs'' (2015) 100 Cornell Law Review 1129; David Partlett, '*New York Times v Sullivan* at fifty years: defamation in separate orbits' in Andrew Kenyon (ed), *Comparative defamation and*

Australia), the point still arises; most recently, the Supreme Court of Canada had to address it in *Goldhar v Ha'aretz*[94] concerning the publication of an article on an Israeli news website concerning a Canadian resident (with business and sporting interests in Canada and Israel).

Again, there can be variation depending on the cause of action; in *CG*, Facebook originally accepted that the Northern Irish courts could hear the action against it, though during the proceedings, it revised its position and challenged the applicability of the Data Protection Act (on the grounds that Facebook Ireland, the data controller, was not established in the UK for the purposes of the Act). While this argument was successful at first instance,[95] and is a familiar defence argument in cases against online services,[96] the Northern Ireland Court of Appeal subsequently found[97] that Facebook (Ireland)'s data processing was carried out in the context of the activities of (UK-established seller of advertising) Facebook (UK). For defamation itself, English law (since 2013) now provides a new test for jurisdiction (that England and Wales be 'clearly the most appropriate place'), albeit only beyond the EU and Lugano states[98] - with the (much more *plaintiff*-friendly) rules of the Brussels Regulation / Lugano Convention, as interpreted by the CJEU,[99] still applying to cases concerning EU and Lugano-domiciled defendants.

Where new legislative obligations are being created, this presents an opportunity to attempt determine in advance how jurisdiction will be addressed. Considering the new obligations reviewed in part 2 above, it can be observed that the tendency is towards casting the net relatively widely. The new 'video sharing platform' category in EU media law, for instance, has a standalone definition of jurisdiction which expressly includes service providers which have either a parent company or a subsidiary that is established on their territory, as well as those which are part of a group where another entity of that group is established on their territory.[100] The Recommendation on Illegal Content adds to existing provisions the inclusion of service providers established anywhere in the world, where the provider directs its activities to consumers residing in the Union.[101] (This is the existing language of the Brussels Regulation on jurisdiction,[102] and so notable for taking something more familiar in the context of private law proceedings and using it in something resembling (albeit voluntary, for the time being) an administrative scheme). The GDPR went beyond the Data Protection Directive in addressing processing outside the EU, where it takes place in the 'context of the activities' of an EU-established controller or processor, or relates to the personal data of EU data subjects in many circumstances.[103] These are of course all different tests, though many intermediaries

---

privacy law (CUP 2016); C Reed, 'Why judges need jurisprudence in cyberspace' (2018) 38 Legal Studies 263.

[94] 2016 ONCA 515.

[95] *CG* (n 60) [91].

[96] See e.g. *Richardson v Facebook* [2015] EWHC 3154 (QB).

[97] Applying CJEU decisions: *Google Spain* (n 85) and Case C-230/14 *Weltimmo v NAIH* [2016] 1 WLR 863.

[98] Iceland, Norway, Switzerland (and EU member Denmark, which is not within the Brussels Regulation).

[99] Case C-509/09 *eDate v X*; Case C-161/10 *Martinez v MGN* [2011] ECR I-10269

[100] AVMSD (n 32), article 28a.

[101] Recommendation on Illegal Content (n 55), para 4(a).

[102] Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, art 17(1)(c).

[103] GDPR (n 82) art 3.

will meet one or more of them and so have to take the law into consideration (even if excluded through analysis of the provisions themselves).

3.4 Law reform

3.4.1 Harms and duties

Current reviews of Internet-related legal issues demonstrate a particular interest in questioning the adequacy of existing measures. Some investigations can be understood as a refocusing of efforts on an underlying phenomenon (e.g. harm through harassment and abuse) rather than the adaptation of the existing causes of action. Others, drawing upon the wider debate on the particular role of intermediaries, are thinking in terms of new duties directed towards intermediaries in order to address issues such as harm to users.

In this section, I identify examples of both trajectories (the former in New Zealand and the latter in the UK), concluding with some cross-cutting challenges that reform initiatives will face, regarding the choices to be made regarding institutions and national borders.

3.4.2 New Zealand

The New Zealand Law Commission carried out a multi-year project on the news media and the new media, following on from a lengthy, four-part project on privacy law where new media issues had been noted but not prioritised.[104] The later review took up technological change as one of its key themes, noting changes in who and how can circulate information. One of its three broad questions was 'whether the existing criminal and civil remedies for wrongs such as defamation, harassment, breach of confidence and privacy are effective in the new media environment and if not whether alternative remedies may be available'.

During the lifetime of the review, the Law Commission provided expedited advice[105] to the NZ Parliament, which reflected this overall approach of going beyond the established causes of action while responding to a specific request (informed by high profile press coverage of abusive and sexually explicit material in private Facebook groups)[106] from the legislature. In turn, Parliament enacted new legislation in the form of the Harmful Digital Communications Act,[107] distinguished by being neither an amendment to existing law nor a new, standalone criminal offence, but an interlocking set of incentives and new remedies.

The HDCA (the relevant provisions of which came into force in 2016) includes both civil and criminal remedies, a complaints handling body (NetSafe), and a set of guiding principles (prohibiting e.g. the disclosure of sensitive personal facts). It also

---

[104] New Zealand Law Commission, *Invasion of Privacy* (NZLC R113, 2010); New Zealand Law Commission, *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC R128, 2013).

[105] New Zealand Law Commission, *Harmful Digital Communications* (NZLC MB3, 2012).

[106] The 'RoastBusters' scandal, dating from 2013 onwards; see Nicola Gavey, *Just Sex? The cultural scaffolding of rape* (2nd edn, Routledge 2018) 229-238.

[107] Harmful Digital Communications Act 2015; see further Ursula Cheer, 'Divining the dignity torts: a possible future for defamation and privacy' in Andrew Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge University Press 2016) 322-329; David Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (Bloomsbury Publishing 2017) 336-341; Savannah Post, 'Harmful Digital Communications Act 2015' (2017) 1 NZ Women's Law Journal 208; Stephanie Frances Panzic, 'Legislating for e-manners' (2015) 21 Auckland University Law Review 225.

has a detailed safe harbour system for intermediaries. The role of the courts includes corrections, rights of reply, takedown notices, and the like, though the intention is that NetSafe deal with complaints in the first instance, with the courts being able to act where NetSafe's requirements have not been complied with, or where its response was not satisfactory.

This shift is, as noted above, towards considering the range of potential harms, without referring directly to existing causes of action or drawing upon their language, defences, and the like. Moreover, the legislation clearly envisages specific but related roles for the regulatory body and for the courts.

3.4.3 UK White Paper

In the United Kingdom, changing attitudes can be found even in the sheer number of reviews asking broad questions about Internet regulation. In Parliament, this has included the House of Lords Communications Committee (asking questions such as 'is there a need to introduce specific regulation for the internet?', and ultimately recommending a set of 10 principles to be pursued by an 'Internet Authority'[108]) and the House of Commons Science and Technology Committee (asking about the impact of social media use by children, and proposing a principles-based regime, new duties, transparency obligations, and a statutory code of conduct[109]). The Government promised legislation that would make the UK 'the safest place in the world to be online'.[110] Doteveryone[111] proposed an 'Office for Responsible Technology' which would, amongst other things, 'support people to find redress' for harms, both individual and collective, related to technology.[112] The Carnegie Trust supported research into 'online harm reduction', with the resulting report recommending a statutory duty of care (which would not replace any existing remedies) and a 'social media harm regulator' (which could be a new function for the existing communications regulator Ofcom).[113]

Most recently, the UK Government has published a white paper on 'online harms'.[114] It is another document with a focus on responsibilities and duties, setting out thoughts on how 'digital products and services [can be] designed in a responsible way, with their users' well-being in mind'[115] and proposing a 'statutory duty of care'

---

[108] House of Lords Select Committee on Communications, *Regulating in a digital world* (HL Paper 299, 2017-19).
[109] House of Commons Science and Technology Committee, *Impact of social media and screen-use on young people's health* (HC 822, 2017-19).
[110] HM Government, *Internet Safety Strategy (Green Paper)* (2017) 2 (foreword by Secretary of State for Culture, Media and Sport Karen Bradley); this document was the first reflection of a manifesto commitment for a digital charter (which would make Britain 'the best place to start and run a digital business' and 'the safest place in the world to be online'): Conservative Party Manifesto (2017) https://s3.eu-west-2.amazonaws.com/conservative-party-manifestos/Forward+Together+-+Our+Plan+for+a+Stronger+Britain+and+a+More+Prosperous....pdf 77. The commitment is also the opening to the 2019 white paper discussed in this section.
[111] A think-tank established by Martha Lane Fox (co-founder of early e-commerce company Lastminute.com, former digital champion appointed by the UK Government, and now member of the House of Lords): www.doteveryone.org.uk.
[112] Catherine Miller, Jacob Ohrvik-Stott and Rachel Coldicutt, 'Regulating for Responsible Technology ' (2018) .
[113] Lorna Woods and William Perrin, 'Online harm reduction – a statutory duty of care and regulator' (*Carnegie UK Trust*, 2019) <https://www.carnegieuktrust.org.uk/publications/online-harm-reduction-a-statutory-duty-of-care-and-regulator/> .
[114] HM Government, 'Online Harms (White Paper)' CP 57.
[115] Ibid 26.

for companies.[116] This duty, echoing though not specifically referring to the mention of duty of care in the ECD,[117] would encompass user safety as well as 'illegal and harmful activity' more generally (though in context, the paper really means illegal *or* harmful activity, given the frequency of references to *legal* harmful activity). A regulatory body would be responsible for creating and monitoring compliance with codes of practice - subject to a comply or explain mechanism, risk-led approaches, and a test of reasonable practicability (akin to aspects of health and safety or financial regulation). In exploring the existing regulatory framework, it notes schemes such as data protection law (which are beyond its scope), though does not refer to criminal law other than in passing,[118] and the focus is clearly on user-generated content and interaction between users (rather than the established, editorial-led media or the classification of films and games). Enforcement options including web blocking, senior management liability, and fines.

The White Paper, and indeed many of the other aforementioned reports and studies, navigate a difficult question of the distinction between 'unlawful' and 'harmful' material. Even where a requirement is confined to unlawful material, distinguishing (as explained in *Delfi*) between content that is obviously illegal and content that necessitates further legal or linguistic assessment in order to establish such illegality[119] may require differing approaches. Moreover, as noted in passing in *Magyar Jeti*, addressing links to unlawful material faces an obvious challenge of changes to material. To these distinctions are added the White Paper's distinction between three categories of content within its scope (clearly defined harms, less clearly defined harms, underage exposure to legal content)[120] and the House of Lords Communications Committee's table of illegal, harmful and anti-social content.

3.4.4 Two design questions

Any new approach will face a number of design and implementation dilemmas. One will be the balance that is struck between judicial (or similar) resolution of disputes and approaches led by a regulatory or administrative agency. The presence of both is not a new issue; a broadcaster, for instance, is accountable to Ofcom for breaches of the Broadcasting Code but can also be a defendant to a tort action in respect of, for instance, defamation or privacy.[121] Moreover, and not without controversy, the agencies or courts responsible for the various blocking schemes in the UK (discussed at 2.3.1, above) already vary; indecent images of children are the concern of the (voluntary) Internet Watch Foundation, copyright infringement addressed by court order (without any regulatory involvement) and the BBFC in line to supervise blocking of non-compliant sexually explicit websites under the Digital Economy Act 2017.

---

[116] Ibid 42.
[117] ECD, recital 42: 'service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities'; recital 48: 'This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to 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'.
[118] Ibid 32-4.
[119] *Delfi* (n 71) [117].
[120] HM Government, 'Online Harms (White Paper)' (n 114) 31.
[121] Recent examples include *Richard v BBC* [2018] EWHC 1837 (Ch), [2019] Ch 169 (privacy) and *Miah v BBC* [2018] EWHC 1054 (QB) (libel).

As noted at 3.4.2, above, a key goal of the New Zealand initiative was to incentivise out-of-court settlement of disputes, especially where swift action rather than compensation is the priority; the same issue has arisen in a review of defamation law in the Canadian province of Ontario,[122] and is familiar in other areas of Internet law (e.g. the global dispute resolution system for domain name disputes[123]). Similarly, the UK reviews have (by and large) focused on the creation of new regulatory structures (using existing agencies or proposing new ones).

A second unavoidable question is whether to proceed on the basis of national boundaries or to think more broadly. One Secretary of State at DCMS told a Commons committee in 2018 that Brexit could allow for the adoption of 'forward looking legislation that supports the innovation and the freedom that (…) social media platforms bring, but also ensure that they mitigate better against the harms'.[124]. Indeed, the repeated rhetoric of making *Britain* the safest place *in the world* to be online underlines this dimension. However, the UK is unlikely to have a completely free hand here, and the level of detail in the white paper regarding interaction with the ECD is minimal,[125] and there is no discussion of newly adopted EU measures or the European Commission's approach to illegal content or disinformation. The ECD is an important component of the EU's single market (as is the more elaborate General Data Protection Regulation, to which the UK remains committed in principle and perhaps by necessity in order to allow for the equivalence necessary to facilitate cross-border data flows). Future negotiations on market access between the UK and the EU will surely see some discussion of the harmonisation of liability or other legal duties which might constitute barriers to trade. Even within the broader body of bilateral and plurilateral trade law (which the UK will show special interest in, post-Brexit), there are examples of intermediary issues being on the table; the proposed new agreement between the US, Mexico and Canada (to replace NAFTA) would, if adopted, require something akin to the (strong) form of immunity under US law (the CDA) across the three parties.[126]

4. Conclusion

> …while it is important to ensure that companies have the right level of liability for illegal content, this is not the most effective mechanism for driving behavioural change by companies[127]

---

[122] Law Commission of Ontario, *Defamation Law in the Internet Age* (consultation paper, November 2017) 120-3; Emily Laidlaw, 'Re-Imagining Resolution of Online Defamation Disputes' (2019) 56 Osgoode Hall LJ 162; Daithí Mac Síthigh, 'Where Do We Go from Here? Reflections on the LCO's Consultation and Conference' (2019) 56 Osgoode Hall LJ 1.
[123] Andrew Murray, *The regulation of cyberspace* (Routledge-Cavendish 2007) 109-113; Jacqueline D. Lipton, *Rethinking cyberlaw : a new vision for Internet law* (Edward Elgar 2015) 108-115.
[124] House of Commons Digital, Culture, Media and Sport Committee, 'Oral evidence: Fake News, and other policy issues connected with the work of the Department' (2017-19) HC 363, Q988 (Matt Hancock).
[125] HM Government, 'Online Harms (White Paper)' (n 114) 9 (non-interference with liability), 61 (desire to 'work with international partners to build consensus and identify common approaches').
[126] Heather Timmons and Hanna Kozlowska, 'Facebook, Google, and Amazon are big winners in the new NAFTA deal' (*Quartz*, 2 October 2018) <https://qz.com/1410473/facebook-fb-google-goog-and-amazon-amzn-are-big-winners-in-the-new-nafta-deal/> .
[127] HM Government, 'Online Harms (White Paper)' (n 114) 62.

The UK Government's recent white paper, which would (if followed through with legislation) confirm broad trends in approaches to Internet intermediaries, proposes new measures rather than amending the law on liability. Indeed, those who are critical of the current position of online content are clearly concentrating their efforts not on amending the general rules on liability, but identifying new ways in which the desired effects can be brought about. In some cases, this may in practice deprive these general rules of much of their commercial and reputational relevance.

In this article, I have highlighted various departures from general liability rules in specific areas (such as media and copyright law), while also arguing that the wide range of recommendations and other instruments contain emerging approaches to the duties and obligations of service providers. In doing so, I am in agreement with Edwards' argument in 2018, that a general narrative against liability (denying moral responsibility and fearing the collapse of the information society) was deconstructed in the 20000s and 'lie(s) in shreds' towards the end of the 2010s.[128] I place particular emphasis, in the evidence presented above, on the cumulative effect of statutory and non-statutory measures, conjoined with press and popular sentiment that is increasingly critical of the power of the technology industries, as relocating arguments regarding responsibility and duty, which would have been unthinkable or at least at the fringes of political debate in earlier years, to the mainstream of media and Internet regulatory conversations.

[128] Edwards (n 1) 286.