Anne Barron

'Graduated response' à l'Anglaise: online copyright infringement and the Digital Economy Act 2010

Article (Submitted version) (Pre-refereed)

Final version available in 2011 3(2) *Journal of Media Law* 305-47
http://www.ingentaconnect.com/content/hart/jml

'Graduated Response' *à l'Anglaise*: Online Copyright Infringement and the Digital Economy Act 2010

Anne Barron
London School of Economics and Political Science

I INTRODUCTION

Since the formation of the first New Labour administration in 1997, the 'creative industries' have moved ever closer to the centre of economic policy-making in the UK.[1] In a context of intense and rising global competition for jobs, tax revenues and export earnings, and the long-term decline of high-volume domestic manufacturing, UK policy-makers have increasingly looked to cognitive and cultural labour as major sources of value for the nation's economy, and have identified intellectual property rights (IPRs) as crucial legal instruments for capturing that value. There is no shortage of scepticism as to whether this strategy could be other than a recipe for legitimising corporate enclosures that diminish the intellectual common, hastening a commercialisation of the arts and culture that will ultimately prove to be self-defeating, and glamorising the precarious and poorly rewarded forms of employment that are endemic within this sector.[2] Yet there is also no sign that the current preoccupation with fostering "the growing success story that is Britain's creative economy"[3] is on the wane: it emerged with renewed vigour from the Blair-Brown Prime Ministerial handover in 2007, and survived the change of Government from New Labour to the Conservative-led coalition in May 2010.[4]

Nonetheless, over the years since 1997, the headline emphasis has shifted from the economic potential of cultural creativity to the manner in which IT-related innovation – as well as generating valuable products and services in itself – could enable UK-produced cultural content to be more effectively exploited at home and abroad.[5] In 2008-9, the Labour Government produced a strategy, entitled *Digital Britain*, for what it now called the UK's 'digital' economy.[6] The premise of the strategy was that the digital economy included both the information and communications technology (ICT)

[1] One of the key documents exemplifying this trend, co-produced by the Department for Culture, Media and Sport (hereinafter DCMS), the Department for Business, Enterprise and Regulatory Reform (hereinafter BERR) and the Department for Business, Innovation and Skills (hereinafter BIS), defines the 'creative industries' to include advertising, architecture, the art and antiques market, crafts, design, designer fashion, film, interactive leisure software, music, the performing arts, publishing, software and computer services, television and radio (DCMS/BERR/BIS, *Creative Britain: New Talents for a New Economy* (February 2008) (hereinafter *Creative Britain*).

[2] See e.g. David Hesmondhalgh and Sarah Baker, *Creative Labour: Media Work in Three Cultural Industries* (London: Routledge, 2010).

[3] *Creative Britain* p.4.

[4] See e.g. BIS/DCMS, "Government Response to the Hargreaves Review of Intellectual Property and Growth" (3 August 2011).

[5] Nicholas Garnham, "From Cultural to Creative Industries" (2005) 11(1) *International Journal of Cultural Policy* 15-29.

[6] BERR/DCMS, *Digital Britain: Interim Report* (London: TSO, 2009) (Cm. 7548); BIS/DCMS, *Digital Britain: Final Report* (London: TSO, 2009) (Cm. 7650).

sector (producing computing and communications equipment and applications) and the 'digital content' sector (producing digitised cultural and informational goods other than software); and that overall it accounted for 10% of UK GDP and 6% of total UK employment.[7] *Digital Britain* was oriented towards ensuring that the UK cultural, media and communications industries could seize the opportunities and manage the risks posed by digital ICTs. Its action plan included modernising and upgrading the UK's digital communications infrastructure (in particular the mobile network spectrum and digital radio); providing a favourable climate for investment and innovation in digital content, applications and services; enabling wider participation in the digital economy by moving towards universal access to broadband and developing the nation's 'digital skills'; and delivering more public services online.

The Digital Economy Bill, introduced in the House of Lords on 19 November 2009, was intended to take forward several of the recommendations in the *Digital Britain* programme that required legislation, but its most controversial provisions related to the use of copyright works online. As originally drafted, these provisions were intended to achieve two goals. The first was to facilitate the further development of markets in digitised content by lowering the transaction costs involved in obtaining licences to use and distribute copyright material. This in turn was to be achieved in two main ways: by making provision for 'extended' collective licensing (extending the powers of collective licensing bodies to works in respect of which their members have no rights), and by making provision for the grant of licences in respect of so-called 'orphan works' (copyright material for which no owner can be found after a diligent search). Whereas these measures were supposed to benefit *users* of copyright material, the second goal of the copyright-related provisions in the Bill was to make it easier for *right-holders* to enforce their rights in the online environment. This was to be achieved primarily by enlisting Internet Service Providers (ISPs) in the project of curbing mass online copyright infringement, for example by means of the peer-to-peer (P2P) file-sharing networks that the UK copyright industries[8] claim cost them in excess of £400 million per annum in lost sales.[9] Summarising its ambitions for the Bill's copyright provisions, the Government declared:

> We want a framework for copyright and performers' rights that reflects the needs of the digital age, and gives the UK's creative industries the chance to develop new legitimate digital products delivered in the way people want, at a price that is fair. That means we need to make doing business easier in this area, and to significantly reduce the amount of online infringement of copyright.[10]

[7] The term 'digital economy' was nowhere defined in either of the reports in which the Digital Britain strategy was explained. A brief explanation of the working assumptions underlying both reports can be found in BIS/DCMS, *Digital Economy Act: Impact Assessments* (April 2010), pp.10-12.

[8] These are industries that to a large extent depend for their profitability on copyright – or more generally, on mechanisms for controlling the replication or repetition of their goods or services. They include the film, TV, music, videogame, software and publishing industries.

[9] BIS/DCMS, *Digital Economy Act: Impact Assessments* p.64. See also British Phonographic Industry, *Digital Music Nation 2010: The UK's Legal and Illegal Digital Music Landscape*.

[10] BIS/DCMS, "Copyright: Factsheet" (November 2009).

In the face of considerable opposition, the provisions on extended copyright licensing and orphan works were dropped from the Bill before it became law on 8 April 2010,[11] although the issues these provisions were designed to address have since been revisited in a major report on the impact of IPRs on innovation and economic growth, commissioned by the Prime Minister in November 2010 and chaired by Ian Hargreaves, Professor of Digital Economy at Cardiff University.[12] The Hargreaves Report, published in May 2011, recommended that the Government facilitate the establishment of a 'Digital Copyright Exchange': a network of interoperable databases of digitised copyright content, providing reliable information about rights ownership and serving as a one-stop-shop for digital rights clearance; it also urged Government to bring forward new legislation providing for extended collective licensing and the licensing of orphan works.[13] By way of a further acknowledgement of the economic case for freeing up the use of copyright material, and echoing the equally wide-ranging Gowers Report on IPRs (2006),[14] Hargreaves in addition proposed some new limits on copyright: the Report recommended 'modernisation' of the array of excepted uses provided for by the Copyright, Designs and Patents Act 1988 (c.48) (hereinafter CDPA), to "reduce transaction costs and stimulate new works in growing sectors of the creative economy."[15] In its response to Hargreaves in August 2011, the coalition Government accepted these recommendations, indicating that it would aim to ensure that a Digital Copyright Exchange was in place by the end of 2012, and would soon bring forward proposals for an orphan works scheme, extended collective licensing and new copyright exceptions.[16]

Meanwhile, whereas the Digital Economy Bill's online copyright infringement provisions survived largely intact to become sections 3-18 of the Digital Economy Act 2010 (c.20) (hereinafter DEA),[17] developments since the Bill's enactment have

[11] The campaign against these provisions was largely driven by professional photographers, concerned to retain their ability to control the use of their images. For a comprehensive summary of the campaigners' objections to the licensing provisions, see http://www.stop43.org.uk/pages/pages/read_more.html.

[12] Ian Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth* (UK Intellectual Property Office, May 2011) (hereinafter Hargreaves Report).

[13] Ibid, Ch. 4. The goal of these measures would be an efficient digital copyright licensing system, where nothing is unusable because the rights owner cannot be found (ibid, p.7).

[14] *The Gowers Review of Intellectual Property* (London: HMSO, 2006).

[15] Hargreaves Report, para. 5.37. The new or extended exceptions should, it was urged, cover 'format-shifting' by consumers (transferring e.g. music purchased on CD to other formats so that it can be played on multiple devices), a wider array of uses for the purposes of library archiving and non-commercial research, and uses of copyright material in parodies (ibid Ch. 5).

[16] BIS/DCMS, "Government Response to the Hargreaves Review of Intellectual Property and Growth."

[17] The other copyright-related measures to survive in the DEA were sections 42 and 43. Section 42 amends the CDPA to equalise the criminal penalties for digital and non-digital infringement of copyright and performers' property rights, and increase the maximum financial penalty that can be imposed on summary conviction of some criminal offences to £50,000. "This is in recognition of the importance of having penalties that are proportionate to the harm caused to UK [creative] industries and which are effective deterrents against infringement" (BIS/DCMA, "Copyright: Factsheet"). Section 43 amends the Public Lending Right Act 1979 to include books in non-print formats (audio books and e-books) in the public lending right scheme, and amends the CDPA to exempt libraries from copyright infringement liability for 'lending' books in non-print formats, thereby removing the need for libraries to negotiate for licences with individual publishers. This "responds to and reflects the changing nature of book publishing and the increasing demand for the loan of books in formats other than print" (BIS/DCMS, "Public Lending Right: Factsheet" (November 2009) available at:

done little to inspire confidence in their likely efficacy. Sections 17-18 DEA pave the way for court orders requiring ISPs to prevent infringing activity *before* it can occur – by disrupting, or blocking altogether, data traffic to and from particular sites (e.g. thePirateBay.org) that are considered to be hubs for infringing activity. Section 17 gives the Secretary of State power to make regulations enabling courts to grant such 'blocking injunctions' at the request of right-holders, but questions would clearly arise as to the compatibility of any such regulations with prevailing EU and domestic rules on freedom of expression, privacy, data protection and the interception of communications. Following advice from OFCOM (the UK's media and communications regulator),[18] the coalition Government decided in August 2011 not to bring forward site-blocking regulations at present on the ground that the framework set up by sections 17-18 DEA was not apt to deliver the outcomes sought by right-holders.[19] The focus of what follows, therefore, is on sections 3-16 DEA, which together institute a new framework for regulating online copyright infringement by end-users of broadband services.

Sections 3-16 lay the foundations for the imposition of new obligations on ISPs providing broadband services (referred to here as Internet Access Providers, or IAPs) to police their subscribers' online activities. First, these sections enable IAPs to be required to notify subscribers when their broadband accounts are alleged by right-holders to have been used to infringe copyright, and to keep records of those subscribers who have received numerous warnings so that right-holders can take targeted legal action against alleged persistent infringers. The Act refers to these as the 'initial obligations', but provides that they only have legal effect when an 'initial obligations code' – made and/or approved by OFCOM with the consent of the relevant Secretary of State[20] and setting out in detail how the obligations must be met – is in force. Second, if the initial obligations fail to curb online infringement

---

http://webarchive.nationalarchives.gov.uk/20100511084737/http://interactive.bis.gov.uk/digitalbritain/2009/12/public-lending-right/).

[18] OFCOM, "Site-Blocking' to Reduce Online Copyright Infringement" (27 May 2011).

[19] "Copyright owners' expectations for a speedy process, with blocks implemented potentially within hours of an application being made, do not appear realistic given the constraints imposed on the Courts by the DEA, the need for a process which is fair to the legitimate interests of site operators and end users, and the practical challenges arising from the current state of site blocking technologies and internet governance" (ibid para. 5.4). However the High Court's recent decision in *Twentieth Century Fox Film Corp. and Ors. v. British Telecom plc* [2011] EWHC 1981 (Ch) (28 July 2011) has since clarified that a species of blocking injunction is already available under s.97A CDPA, albeit of narrower scope than the orders envisaged under ss. 17-18 DEA. Further, according to the OFCOM report on site-blocking, other strategies for cutting off the supply of unlawful content on the Internet remain actively under consideration. It seems likely that these will include government brokering of arrangements between industry players whereby online intermediaries 'voluntarily' undertake to play a more active role in preventing copyright infringement *ex ante* (see Peter Bradwell, 'Right-Holders' Proposed Voluntary Website Blocking Scheme', 22 June 2011, www.openrightsgroup.org/blog/2011/rights-holders-propose-voluntary-website-blocking-scheme). Such a move would be in line with developments elsewhere in recent years: see generally Jeremy de Beer and Christopher D. Clemmer, "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?" (2009) 49 *Jurimetrics* 375, and for a critical assessment of proposed US measures (widely referred to as 'SOPA' and 'PIPA') exemplifying an enforcement policy broadly similar to that in ss 17-18 DEA, see Mark A Lemley, David S Levine and David G Post, 'Don't Break the Internet' (2011) 64 *Stanford Law Review Online*, 34-38.

[20] It was initially envisaged that the Secretary of State for Business, Innovation and Skills would be responsible for overseeing the implementation of the DEA, but responsibility for the policy area that includes the DEA was moved to the DCMS in December 2010.

significantly, IAPs may in the future be required to take 'technical measures' (which may include capping connection speeds, bandwidth-throttling and disconnection) against subscribers who are alleged to be persistent infringers. The Act refers to these as the 'technical obligations'. Together, the initial and technical obligations envisage a 'graduated response' by IAPs to allegations by right-holders of infringing activity by subscribers: an escalating series of warnings and sanctions, possibly culminating in disconnection from the Internet. To this extent the DEA mirrors initiatives already taken or under consideration in several other countries, and it is clear that UK policy-makers were influenced to some degree by the French 'Création et Internet' legislation,[21] which was first presented to the French Senate in June 2008 and finally came into force in 2010 (though only after a challenge to its constitutionality forced a re-think).[22] None of the envisaged obligations depends on IAPs already being liable as a matter of private law for the activities of their subscribers, nor does the DEA impose such liability. Rather, the obligations in principle affect all IAPs, as defined, simply by virtue of being IAPs – although the Act anticipates that secondary legislation will limit their application to IAPs with the largest shares of the broadband market. Effectively, then, the largest IAPs will be required to assist copyright owners in the enforcement of the latter's private rights against those of their own customers who infringe copyright online, even when they are not themselves liable as accessories to these customers' infringements. These IAPs will also have to bear a substantial share of the total monetary cost of the new enforcement regimes, although most of that cost will be borne by right-holders.

The implementation of the initial obligations regime has, however, been a tortuously slow process. The immediate reason for the delay has been a judicial review which led to the re-drafting of the two key pieces of secondary legislation required to bring the initial obligations into effect. One of these is the order by which OFCOM makes the initial obligations Code; the other is the (necessarily prior) order by which the Secretary of State specifies how that Code must provide for the apportionment of the cost of the initial obligations regime as between copyright owners, IAPs and, in the case of subscriber appeals, the subscriber concerned. First drafts of both measures were initially published in mid-2010. A second draft of the cost-sharing order was not finalised until June 2011, and at the time of writing a second draft of the Initial Obligations Code is still awaiting the Secretary of State's approval. However, because

[21] "Consultation document on legislative options to address illicit P2P file-sharing" (July 2008), Annex C.

[22] See Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet [Law No. 2009-669 of June 12, 2009 Favouring the Diffusion and Protection of Creation on the Internet], amended Sept. 15, 2009, Journal Officiel de la République Française, available at http://www.assembleenationale.fr/13/pdf/ta/ta0332.pdf. The legislation originally gave an administrative authority power to order IAPs to disconnect subscribers who were suspected of repeat infringements for a period of up to one year, and to 'blacklist' these subscribers for an equivalent period so that no other French IAP could provide an alternative connection. The French Constitutional Council took the view that freedom to access the Internet was included in the French Constitution's protection for the freedoms of expression and communication, and condemned the application of the sanction of disconnection by an administrative authority as inconsistent with the presumption of innocence and the right to due process (see decision no. 2009-580DC, Journal Officiel de la République Française (June 10, 2009), available at www.conseil-constitutionnel.fr/decision.42666.html). Consequently, the legislation was amended to require a judicial hearing before disconnection could occur.

both measures are covered by the Technical Standards Directive (TSD),[23] both are required to be notified to the European Commission under Article 8(1) TSD before being laid before Parliament; and Article 9(1) TSD requires that their adoption be postponed for three months from notification so that the Commission and other Member States may consider whether they create obstacles to the free movement of services in the EU. The cost-sharing Order has already been so notified; the Code will be notified when approved. Once laid, the negative resolution procedure applies to the latter; but the lengthier affirmative resolution procedure applicable to the former requires that it meet with the positive approval of each House, rather than no decision to annul it, before it can come into effect.

Unquestionably, however, a further reason for the slow pace of the implementation process is a growing lack of confidence in the online copyright infringement provisions of the DEA – either because of their perceived incompatibility with fundamental rights, or because of their likely inefficacy as a tool of economic policy. Ever since the Bill was first introduced, these provisions have attracted trenchant criticism from civil liberties and consumer rights advocates, and IAPs. All of these critics expressed concern about the limited Parliamentary scrutiny received by the Bill before it became law, and about the prevalence in sections 3-18 of skeleton powers and other provisions delegating legislative power to the Secretary of State or to OFCOM. Civil liberties groups have in addition raised concerns about the implications for data protection of the proposed process for identifying and retaining information about subscribers who have allegedly infringed copyrights, about the reliability of the evidence that would trigger action against alleged infringers, about the effects on privacy and freedom of expression of disrupting or disconnecting the Internet accounts of alleged infringers, about the absence of provision for a court hearing before these sanctions would be administered, and about the danger of effectively subjecting legitimate content to private forms of censorship. Proponents of 'Internet freedom' have in addition pointed to the risk that the principle of 'Net neutrality'[24] will be breached if traffic management tools[25] are deployed by IAPs in favour of copyright owners. Consumer groups have argued that mass online copyright infringement is an inevitable consequence of the cultural industries' failure to meet consumer demand for affordable content in a variety of user-friendly formats.

[23] Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L204, as amended by Directive 98/48/EC [1998] OJ L217.

[24] The principle of 'Net neutrality' in its purest form assumes that there should be no discrimination between types of data traffic by network operators; and that those delivering content, applications and services via the Internet should not be charged by ISPs for the distribution of that content to ISPs' subscribers. The term was coined by Tim Wu: see Tim Wu, "Network Neutrality, Broadband Discrimination" (2003) 2 *Journal of Telecommunications and High Technology Law* 141-79.

[25] The term 'traffic management' refers to a range of techniques that may be used by ISPs to prioritise some types of Internet traffic over others, which may be degraded, throttled, or blocked altogether. Filtering technologies, for example, "can identify particular types of file (e.g. music files), check whether the file is subject to copyright protection and then check whether the person offering the file for download has the right to do so. If no such permission is found, the filter can block the download" (BERR, "Consultation document on legislative options to address illicit P2P file-sharing" (July 2008), para 7.10). Even techniques that aim to filter only unlawful content are regarded by many advocates of Net neutrality as immediately suspect as threatening civil liberties (because of the risk that legitimate sites and content will be automatically blocked) and at odds with the Internet's essential nature as "a decentralized network, in which no party can unilaterally decide to block the information flowing through the communications architecture" (http://www.laquadrature.net/en/Net_Filtering).

Meanwhile, IAPs are divided. Only the seven largest UK IAPs (accounting for around 90% of the broadband access market) will be caught by the new obligations, and they are concerned that many of their subscribers will migrate to smaller IAPs to whom the obligations do not apply. Some major IAPs – notably those with substantial content interests – have expressed support for the Act.[26] However one (TalkTalk), led a campaign against the online copyright provisions of the Digital Economy Bill[27] and, along with another major IAP (British Telecom), mounted the legal challenge to sections 3-18 of the Act to which brief reference was made above.

These concerns about the online copyright infringement measures might have been predicted, but recently criticism has emerged from more surprising quarters. In May 2011, the U.N. General Assembly published the Report of the Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.[28] The Rapporteur emphasised that international norms affecting this right were fully applicable to Internet communications; that facilitating access to the Internet and to online content, with as few restrictions as possible, should be a priority for all States; and that while States bore the primary duty to protect human rights, there was a risk that the Internet's private sector gatekeepers (especially ISPs) might assist, or become complicit with, violation by States of the right to freedom of expression online. The measures indicted by the Report as threatening the right included disconnection of users for the breach of others' IPRs – a measure which the Rapporteur concluded would necessarily be disproportionate and thus a violation of Article 19(3) of the International Covenant on Civil and Political Rights.[29] The Rapporteur accordingly expressed 'alarm' at "legislation based on the concept of 'graduated response' … such as the so-called 'three strikes law' in France and the Digital Economy Act 2010 of the United Kingdom;"[30] and he recommended that all such legislation be repealed.[31]

While this report found graduated response legislation wanting from a human rights perspective, the Hargreaves Report was less than enthusiastic about its economic benefits. Though not going so far as to recommend the repeal of the DEA, Hargreaves sent a clear message to Government that stringent enforcement measures were unlikely on their own to have a significant impact on the incidence of online copyright infringement, and could even damage the digital economy if designed or implemented in a way that alienated consumers.[32] In this, Hargreaves echoed the arguments of the

[26] See Emma Barnett, "Digital Economy Act: TalkTalk and BT Mount Legal Challenge" *The Telegraph*, 8 July 2010 (http://www.telegraph.co.uk/technology/news/7878680/Digital-Economy-Act-TalkTalk-and-BT-mount-legal-challenge.html).
[27] See http://www.dontdisconnect.us/
[28] A/HRC/17/27.
[29] Ibid para. 78. In June 2010, the European Data Protection Supervisor had already expressed the view that three strikes disconnection policies involved disproportionate interferences with the right to privacy and data protection under EU law and the European Convention on Human Rights (Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement, 2010/C 147/01, para. 31).
[30] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n28), para. 49.
[31],Ibid para. 79.
[32] Hargreaves Report para. 8.45. The Report cautioned that the available statistics on the scale of digital piracy and its true impact on growth and incentives in the creative industries were unreliable, and that the evidence of the impact of stronger enforcement on levels of online piracy was inconclusive (paras.

many business analysts and copyright industry observers who have warned that the industries' attempts to fight online copyright 'piracy' with nothing other than stronger enforcement measures are doomed. Rather than persist with futile efforts to control the use of digitised content on the Internet, they are increasingly being urged to accept that giving content away for free can generate more value than locking it up, and to develop mechanisms for monetising this value by means other than metering usage and levying copyright royalties.[33] Sections 3-16 DEA, on the other hand, reflect an assumption that mass online copyright infringement poses a major threat to the cultural industries, that it can and must be significantly reduced, and that the best way to achieve this is by obliging IAPs to police their subscribers' Internet usage.

This Article undertakes a detailed and comprehensive examination of these provisions with a view to illuminating their context and revealing the conflicts they have generated – conflicts that continue to yield challenges both to their legality and to their legitimacy, and could yet make them a dead letter. Part 2 below identifies the regulatory strategy embodied in the provisions, the legal context that frames them, and the background to their inclusion in the DEA. Parts 3 and 4 analyse the details of the initial and technical obligations regimes (in so far as these are known) respectively. Part 5 considers the arrangements for covering the monetary cost of implementing these regimes. Part 6 concludes.

2 INTERNET ACCESS PROVIDERS, THE COPYRIGHT INDUSTRIES AND THE 'DIGITAL ECONOMY'

2.1 Copyright Enforcement as Network(ed) Regulation

'Better' regulation (as distinct from 'de-'regulation) has been the stated aim of the UK Government's regulatory activity since the incoming Labour administration's launch of the Better Regulation Task Force (BRTF) in 1997.[34] Signalling a departure from the avowedly anti-regulatory ideology that had taken root in the 1980s, this approach sought a third way between outright hostility to, and unquestioning support for, regulatory intervention in economic affairs.[35] In several influential reports, the BRTF repeatedly urged governments to consider a range of regulatory strategies before intervening in a given domain of economic activity.[36] It and its successors have

8.9-8.39). The DEA's enforcement measures, Hargreaves recommended, should be carefully monitored so that the approach can be adjusted in the light of new evidence. There is even a suggestion in the Report that these measures might be held in reserve for right-holders whose works are held in the proposed Digital Copyright Exchange and therefore available for licensing (para 4.34).

[33] See e.g. Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006); Don Tapscott and Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything* (2nd ed. (London: Penguin, 2008) p.279.

[34] The BRTF was replaced by the Better Regulation Commission in 2006, which was in turn replaced in 2008. The coalition Government has retained a version of the better regulation agenda: see http://www.bis.gov.uk/policies/bre/better-regulation-framework.

[35] For critical appraisals of the phenomenon, see the essays collected in Stephen Weatherill (ed.) *Better Regulation* (Oxford: Hart 2007).

[36] See especially *Self-Regulation: Interim Report* (London: Cabinet Office, 1999), *Alternatives to State Regulation* (London: Cabinet Office, 2000), and *Imaginative Thinking for Better Regulation* (London: Cabinet Office, 2003).

repeatedly emphasised that top-down, heavy-handed, prescriptive regulation can fail to achieve its goals, impose costs that outweigh its benefits, and generate unintended consequences that exacerbate the problems prompting calls for regulation in the first place. Hence they have urged Government to use this 'classic' regulatory strategy only as a last resort, and then only if it can be shown that the risks of regulatory failure had been taken into account and accommodated and that it is likely to be more effective than other means such as information and education campaigns (urging regulatees to change their behaviour of their own accord), economic incentives (for example via taxes that in effect raise the price of undesirable behaviour, but do not prohibit it) and self-regulation or co-regulation.

Self-regulation has tended to be understood by UK policy-makers and proponents of better regulation as a process whereby 'industry' – typically a collective of actors involved in a particular industry (e.g. firms, or sectoral representatives) – takes initiatives to devise and enforce industry codes of practice, either without government involvement, or with only limited involvement by government (for example as a facilitator of negotiations). Thus while on this understanding self-regulation is consistent with intentional rule-making, these rules are self-formulated, self-enforced and hence 'soft' (not legally binding). Co-regulation, on the other hand, is self-regulation backed up in some way by government action. The central case of co-regulation is rule-making or standard-setting by industry, coupled with some form of legislative underpinning for these rules or standards.[37] Legislation might, for example, delegate power to industry to devise and enforce a code of practice regulating action in a particular domain (perhaps with the mandatory involvement of other affected actors, or 'stakeholders', and subject to formal approval by a regulatory agency), and equip the relevant Secretary of State with a backstop power to impose one if no code is produced voluntarily. OFCOM sees self-regulation and co-regulation as occupying points on a spectrum, the latter being an extension of the former and involving "both industry and the government (or regulator) administering and enforcing a solution in a variety of combinations. Thus the aim is to harness the benefits of self-regulation in circumstances where some oversight by OFCOM may still be required."[38] Advantages associated with both self- and co-regulation are said to include higher levels of commitment to regulatory rules that regulatees perceive as 'theirs' and hence grounded in reliable information and less intrusive than rules formulated by government, lower costs (because industry has a relevant expertise or capacity not available to government), and flexibility (because rules can easily be adapted to meet changing circumstances).[39]

When illegal file-sharing was first officially identified as a problem requiring a regulatory solution, the hope was expressed that IAPs and content providers would work together to agree processes and mechanisms for dealing with it, thereby making

[37] "Codes of practice that are negotiated and enforced within the industry are known as self-regulation, while those that have a statutory backing or other significant Government involvement are called co-regulation" (BRTF, *Imaginative Thinking for Better Regulation* p.41).
[38] BERR, "Consultation document on legislative options to address illicit P2P file-sharing" (July 2008), Annex E, p. 49.
[39] See e.g. Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* 2nd ed. (Oxford: OUP, 2012) Ch. 8; Anthony Ogus, "Rethinking Self-Regulation" (1995) 15(1) *Oxford Journal of Legal Studies* 97.

it unnecessary for government to legislate at all.[40] As will be shown in Part 2.3 below, this hope faded as New Labour's anti-piracy strategy moved through the various iterations generated by successive public consultations, amendments to the Digital Economy Bill as it progressed through Parliament, and events subsequent to the Bill's becoming law. With the prospect of industry self-regulation receding, a co-regulatory solution was then sought. However when this too failed to materialise, what emerged in the Bill – and was subsequently encoded in sections 3-16 DEA – was a strategy of 'networked' regulation[41] of online uses of copyright material. As Parts 3 and 4 below reveal, the legislation is calculated to mobilise a variety of non-governmental actors – right-holders, IAPs, and even subscribers whose broadband accounts might be used to infringe without their knowledge – towards monitoring Internet users' activities and identifying and curtailing infringing activity; and in so doing it will trigger the deployment of a wide variety of 'regulatory' techniques.[42] Right-holders will have an incentive to refine their technological tools for tracking online activity. The initial obligations will require IAPs to use their own information about subscribers' Internet usage to assist copyright owners in singling out individuals deemed particularly threatening to right-holder interests for targeted warnings and legal sanctions. The technical obligations will, if introduced, require IAPs *physically* to curb their subscribers' online activities, *without* the cases against them necessarily being tested by a Court or other tribunal. Further, the introduction of these obligations will in turn be contingent on right-holders taking other steps to undermine the 'culture of piracy' on the Web. The copyright industries will have to show that they have made efforts to change consumers' attitudes to copyright law and educate consumers about the damage done by infringing activity online. They will also have to show that they have made progress towards providing consumers with access to a wider array of alternative, lawful, sources of online content. Here lies a clue to what may well be the ultimate goal of the DEA's online copyright infringement provisions. If the copyright industries are to be able to point to lawful alternatives to file-sharing, they must develop new online distribution channels for their content. Sections 3-16 DEA thus seem calculated to nudge the copyright industries and the broadband industry into new forms of alliance,[43] whereby particular IAPs would not only provide Internet access but would be paid to deliver particular providers' content to their own subscribers on preferential terms.[44] The underlying assumption seems to be that a restructuring of the online content marketplace along these lines would boost the development of the digital economy.

[40] *The Gowers Review of Intellectual Property* paras 5.92-5.100.

[41] There are huge literatures on the phenomenon of networked governance, each offering different perspectives on how the phenomenon can be understood. For an appropriation of some of these perspectives for an account of 'post-regulatory' regulation, see Julia Black, "Decentring Regulation: The Role of Regulation and Self-Regulation in a 'Post-Regulatory World'" (2001) *Current Legal Problems* 103-46.

[42] Difficulties clearly attend the labelling of non-legal and non-state instruments of behaviour management as 'regulatory', but not naming them as such risks obscuring the true breadth of the strategy under discussion here.

[43] This intention is vaguely hinted at in various pre-DEA policy documents, e.g. *Creative Britain* (at paras. 5.1-2; and BERR, '"Consultation document on legislative options to address illicit P2P file-sharing" (July 2008) at p.30.

[44] This of course could in itself have further implications for network neutrality, as IAPs could seek to block or degrade even the legitimate content of rival producers. For an analysis of the regulatory issues arising in the US context from the interaction of the provision of Internet access and specialised services, see James B Speta, "Supervising Managed Services" (2011) 60 *Duke Law Jnl.* 1715.

None of the foregoing is to be taken as suggesting that the DEA regulates a previously unregulated zone. The allocation by the State of private rights such as copyrights is itself a regulatory strategy oriented towards incentivising behaviour deemed desirable and constraining that deemed undesirable, and the bundle of rights comprised in a copyright already includes rights – such as the right to control the copying and transmission of copyright material – covering those online activities that are currently considered to be undermining the cultural industries. However the new provisions emerged from a perception that this strategy was simply ineffective to prevent unauthorised file-sharing (currently the most significant form of mass online infringement), chiefly because the costs associated with invoking private rights against this activity are prohibitively high. Copyright owners can locate the Internet Protocol (IP) addresses of unauthorised uploaders of their copyright works circulating in file-sharing networks relatively easily: initiating a download of this material will cause the uploader's IP address to be revealed to the downloader. However, right-holders cannot unilaterally identify the Internet users to whom those IP addresses have been allocated. This information is only held by the user's ISP, and the ISP cannot pass this information on to the copyright owner without a court order: specifically, a *Norwich Pharmacal* order.[45] Once a court order has been obtained, right-holders are in a position to institute proceedings for copyright infringement against the named individual, but they have in the past been deterred from incurring the costs of legal action because they have lacked a reliable means of distinguishing frequent from occasional infringers using IP addresses alone, these generally being dynamic – changing each time a subscriber logs on. Since each infringing act of 'sharing' is typically of low value (and right-holders estimate that there are some 6.5 million people in the UK who are active unlawful file-sharers),[46] it has not been practical or economic for copyright owners to investigate which IP address is associated with each and every such act, apply for court orders to identify the perpetrators, and bring civil suits against each one. Meanwhile, it is unclear whether copyright liability for file-sharing extends beyond the individual uploaders and downloaders who participate directly in file-sharing networks, and if so, how far.[47] The result of these difficulties, in the view of the cultural industries and the Government, has been a particular kind of market failure. Property rights in the digitised copyright material that circulates through file-sharing networks have become virtually unenforceable, with the result that 'free-riding' on this material – the obtaining of benefits from it by those who have not shared in the cost of producing it – has become rife. Unless curtailed, it is said, the result of such rampant externalities will be ever-decreasing profits for the cultural industries, leading in turn to loss of employment and declining tax revenues.[48]

[45] *Norwich Pharmacal Co. v. Commissioners of Customs and Excise* [1974] AC 133; see now CPR, rule 31.18.
[46] BIS/DCMS, *Digital Economy Act: Impact Assessments* p.56.
[47] Haflidi Kristjan Larusson, "Uncertainty in the Scope of Copyright: The Case of Illegal File-Sharing in the UK" (2009) EIPR 124.
[48] BIS/DCMS, *Digital Economy Act: Impact Assessments* pp. 58-59. This account of the impact of file-sharing has been contested: see e.g. Felix Oberholzer-Gee and Koleman Strumpf, "The Effect of File Sharing on Record Sales: An Empirical Analysis" (2007) 115 *J.Pol.Econ.* 1; and Annelies Huygen et al., *Ups and Downs: Economic and Cultural Effects of File Sharing on Music, Film and Games* (TNO, 2009). So divergent are the statistics that the Hargreaves Review concluded in May 2011 that it is "difficult to reach confident conclusions" about the impact of digital copyright piracy (Hargreaves, *Digital Opportunity* p.73).

The DEA's provisions on online copyright infringement reflect a conviction that IAPs have capacities and resources that could help to solve this problem, but have failed voluntarily to accept responsibility for contributing to a solution and should now be compelled to do so.

2.2 The Domestic, EU and International Legal Context

The reasons for IAP inaction are not difficult to fathom. Typically, the contract between an ISP and its subscribers prohibits the subscriber from using the service for unlawful purposes, but UK IAPs have had few incentives to enforce this contractual term against subscribers who infringe copyright. The main reason is that although UK copyright law recognises a concept of accessory liability,[49] EU law (in the shape of Article 12 of the E-Commerce Directive)[50] requires that IAPs be given substantial immunity from liability for merely supplying the 'pipes' through which infringing digital content passes.[51] IAPs have therefore not been inclined to take action against subscribers alleged to be using their Internet services unlawfully to download or transmit copyright material. A less extensive safe harbour must, under Article 14 of the E-Commerce Directive,[52] be granted to ISPs (such as YouTube) that host or store content at the request of subscribers – less extensive because it is conditional on hosts taking action once they acquire knowledge that content is being stored unlawfully. Still, this has effectively placed the burden on copyright owners to find infringing material and inform the ISP of its existence on its network, and even then the maximum extent of the ISP's duty has been to remove, or disable access to, the allegedly infringing material. Under Article 15, meanwhile, Member States are prohibited from imposing on ISPs a general obligation to monitor the information that they transmit or store. Similar immunities have long been available under the laws of other jurisdictions.[53]

Since 2008, however, 'graduated response' regimes – often called 'three strikes' regimes[54] – have mushroomed across the globe, some entirely dependent on private

[49] See e.g. CDPA s.16(2) (defining primary liability for 'authorising' any of the acts exclusively reserved to the copyright owner), and ss. 22-27 (defining secondary liability for certain acts done in relation to acts of primary infringement).

[50] Directive 2000/31 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (8 June 2000) [2000] OJ L178.

[51] Article 12 of the E-Commerce Directive defines a 'safe harbour' for providers of services that consist in the provision of access to a communication network (e.g. via a broadband connection), or the automatic transmission of third party content through a network (e.g. by email). Member States are obliged to immunise providers from any liability for damages and criminal penalties which would otherwise arise from acting as a 'mere conduit' for (i.e. merely transmitting) information. The conditions attached to this immunity are that the ISP (a) did not initiate the transmission in issue, (b) did not single out the recipients of the transmission except by way of an automatic response to the request of another person and (c) exercised no editorial function in relation to the information transmitted. Regulation 17 of the Electronic Commerce (EC Directive) Regulations 2002 (S.I. 2002/2013) (hereinafter E-Commerce Regulations) implements Article 12 in the UK.

[52] This has been transposed into UK law by regulations 19 and 22 of the E-Commerce Regulations.

[53] See e.g §512 US Copyright Act 1976 (Pub. L. 94-553, 90 Stat. 2541 19 October 1976) (17 U.S.C.), as inserted by the Digital Millennium Copyright Act 1998 (Pub. L. 105-304, 112 Stat. 2860, 28 October 1998).

[54] The graduated response strategy is often referred to as a 'three strikes and you're out' approach to online copyright infringement, on the basis that disconnection usually occurs after three warning letters have been ignored.

arrangements between right-holders and ISPs;[55] others buttressed by legislation or judicial decisions.[56] Meanwhile, negotiations over the terms of a new international agreement on the enforcement of IPRs – the Anti-Counterfeiting Trade Agreement (ACTA) – appeared likely for a time to culminate in a requirement that signatory Parties legislate for, or at least encourage the voluntary adoption of, both graduated response schemes and proactive copyright enforcement by IAPs. A draft 'internet enforcement chapter' (dated 30 September 2009) mooted rules requiring ACTA signatories to replicate U.S. law by making ISP safe harbours conditional on their "put[ting] in place policies to deter unauthorised storage and transmission of … infringing content [for example] clauses in customers' contracts allowing, inter alia, a graduated response."[57] This in turn prompted a worldwide coalition of consumer groups, civil liberties NGOs, ISP industry associations and Web 2.0 firms to produce an open letter[58] expressing concern about both the process and substance of the negotiations.[59] As to substance, the letter charged that the proposed Internet enforcement chapter could hinder innovation while undermining fundamental rights, especially freedom of expression and communication privacy. In a resolution passed in March 2010, the European Parliament also expressed its concern over the lack of transparency in the ACTA negotiations to that point, and called for an assessment of ACTA's projected impact on fundamental rights. In particular, the resolution articulated the Parliament's view that "in order to respect fundamental rights, such as the right to freedom of expression and the right to privacy … the proposed agreement should not make it possible for any so-called 'three-strikes' procedures to be imposed" and that "any agreement must include the stipulation that the closing-off of an individual's Internet access shall be subject to prior examination by a court."[60]

[55] The efforts of the Record Industry Association of America (RIAA) in this regard have been particularly well publicised: (see e.g "RIAA CEO Encourages ISPs to Work with Music Industry to Address Digital Theft" (RIAA press release, 6 May 2008, and Greg Sandoval, "Top ISPs Poised to Adopt Graduated Response to Piracy", June 22 2011, http://news.cnet.com/8301-31001_3-20073522-261/exclusive-top-isps-poised-to-adopt-graduated-response-to-piracy/. It is certainly within the power of US ISPs to design their terms of use to enable them to suspend access to their services in cases of suspected repeat infringement, and some have: see Annemarie Bridy, "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement" (2010) 89 *Oregon Law Review* 81.

[56] At the time of writing, such legislation has been enacted in France, New Zealand, South Korea and Taiwan, as well as the UK. For an analysis of relevant Australian case law, see Robert Burrell and Kimberlee Weatherall, "Providing Services to Copyright Infringers: *Roadshow Films Pty Ltd v iiNet Ltd*" (2011) 33 *Sydney Law Review* 723.

[57] European Commission "ACTA Negotiations – Internet Chapter" (Ref. 588/09) (available at: http://www.laquadrature.net/wiki/ACTA_Draft_Internet_Chapter). (§ 512(i)(1)(A) of the US Copyright Act conditions its safe harbours on the ISP having "a policy that provides for the termination in appropriate circumstances of subscribers … who are repeat infringers.")

[58] http://freeknowledge.eu/acta-a-global-threat-to-freedoms-open-letter

[59] ACTA negotiations occurred outside the framework of existing institutions such as the World Intellectual Property Organisation and the WTO, and largely in secret, prompting concerns about the transparency of the process.

[60] European Parliament Resolution on the transparency and state of play of the ACTA negotiations, 10 March 2010 (P7_TA(2010)0058). See also the Parliament's Resolution on Cultural Industries in Europe, 10 April 2008 (P6_TA(2008)0123), urging EU Member States "to avoid adopting measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access."

A consolidated draft text of ACTA – released for public discussion in April 2010[61] – contained no provisions requiring signatories to *direct* ISPs to introduce either graduated response or filtering/blocking regimes. Instead the text identified 'options' for consideration by the negotiators that would have allowed Parties to legislate for such regimes, and would have required signatories eschewing compulsion to promote their voluntary development instead.[62] The finalised text published on 3 December 2010[63] was further diluted. It commits each Party to ensuring that enforcement procedures are available against infringements of IPRs taking place online, but also to ensuring that these are implemented "in a manner that avoids the creation of barriers to legitimate activity, including electronic commerce, and … preserves fundamental principles such as freedom of expression, fair process, and privacy."[64] Further, it contains no commitment to promote graduated response regimes as such, only an undertaking to "endeavour to promote cooperative efforts within the business community to effectively address … copyright or related rights infringement while preserving legitimate competition and consistent with each Party's law, preserving fundamental principles such as freedom of expression, fair process, and privacy."[65]

Of course nothing in ACTA prevents signatory Parties from electing, as the UK has, to enact legislation imposing graduated response regimes, although EU Member States taking this route must comply with applicable EU law. Nothing in the Directive on the Enforcement of IPRs[66] specifically prevents or authorises the measures set out in the DEA,[67] although the European Commission has in the last three years been responding to the concerns of national authorities and 'stakeholders' about the increasing incidence of IPR infringement, including online copyright infringement. One of its initiatives has been to encourage talks between those affected by unlawful file-sharing with a view to securing voluntary cooperation within the existing legal framework.[68] In December 2010 the Commission reported that the Enforcement Directive "was not designed with the challenge posed by the Internet … in mind"[69] and suggested that "[g]iven intermediaries' favourable position to contribute to the prevention and termination of online infringements, the Commission could explore how to involve them more closely."[70] A review of the Enforcement Directive is expected in early 2012.

---

[61] ACTA "Consolidated Text Prepared for Public Release", available at: http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf.

[62] Ibid, Article 2.18 para. 3*quater*: "Each Party *shall* promote the development of mutually supportive relationships between online service providers and right holders to deal effectively with … copyright or related rights infringement which takes place by means of the Internet, including the encouragement of establishing guidelines for the actions which should be taken" (emphasis added). See also Annemarie Bridy, "ACTA and the Specter of Graduated Response" (2011) 26(3) *Am. Law Rev.* 558-77.

[63] http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf.

[64] ACTA Article 27 paras. 1 and 2.

[65] Ibid. para. 3

[66] Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L157.

[67] Consequently, legal arrangements for dealing with online copyright infringement vary considerably among the Member States: for an overview, see Commission Staff Working Document, "Analysis of the Application of Directive 2004/48/EC in the Member States" SEC (2010) 1589 final (22 December 2010).

[68] See European Commission, "Synthesis Report on the Stakeholders' Dialogue on Illegal Up- and Downloading 2009–2010" (March 2011).

[69] European Commission, "Report on the Application of Directive 2004/48/EC on the Enforcement of Intellectual Property Rights" COM(2010) 779 final (22 December 2010), p.9.

[70] Ibid. p.7.

At present, however, the relevant EU law comprises the E-Commerce Directive referred to above, together with the so-called 'Telecoms Package' – the EU's regulatory framework for electronic communications networks and services. Implemented in 2003 with the aim of making the electronic communications sector in the EU more competitive, the package comprises a general 'Framework' Directive[71] and four specific Directives. The 'Authorisation' Directive[72] harmonises and simplifies the process by which national regulatory authorities confer entitlements to provide electronic communications networks and services. Its main innovation was to require Member States to replace individualised licensing arrangements with 'general authorisation schemes': general conditions of entitlement to provide networks and services. The 'Access' Directive[73] harmonises how Member States regulate the terms on which providers may access, and/or interconnect with, each other's networks and services. The 'Universal Service' Directive[74] requires Member States to ensure that a minimum set of electronic communications services of a certain quality (including e.g. a connection to a public telephone network that allows functional Internet access) is made available at an affordable price to all end-users. Finally, the 'Privacy and Electronic Communications' Directive[75] translates the principles of the Data Protection Directive[76] into specific rules for the electronic communications sector. Given their particular importance in regulating the operation of graduated response regimes, the provisions of these two Directives will be briefly elaborated here.

The Data Protection Directive (DPD) regulates the processing of individuals' personal data. "Personal data" is defined as "any information relating to an identified or identifiable natural person."[77] Thus data are 'personal' when it is reasonably possible to link the information to a person (the 'data subject'), even (arguably) if the holder of the data cannot make this link.[78] 'Processing' in the context of the DPD means 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and includes collection, storage, dissemination and blocking.[79] The DPD provides that Member States' implementing legislation must apply the Directive's requirements to the 'controller' of this processing, defined as 'the natural or artificial person … which alone or jointly with others determines the purposes and means of' the processing.[80] Article 6 requires Member States to provide that personal data may only be collected for specified, explicit and legitimate purposes, and not

[71] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services [2002] OJ L108.
[72] Directive 2002/20/EC on the authorisation of electronic communications networks and services [2002] OJ L108.
[73] Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities [2002] OJ L108.
[74] Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services [2002] OJ L108.
[75] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201.
[76] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281.
[77] DPD, Article 2(a)
[78] See e.g Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, (WP136), 20 June 2007 (adopting a broad interpretation of 'personal data').
[79] DPD, Article 2(b).
[80] Ibid Article 2(d).

further processed in a way incompatible with those purposes; and that any processing be relevant and proportionate to the purpose pursued. Article 7 lists among the purposes that qualify as legitimate those of: ensuring the performance of a contract to which the data subject is party; ensuring compliance with a legal obligation to which the controller is subject; ensuring performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; and protecting the legitimate interests of the controller or a third party to whom the data are disclosed (except where such interests are overridden by the fundamental rights and freedoms of the data subject, and in particular the right to privacy). Under Article 8, extra restrictions apply to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and details of the subject's health or sex life. The provisions of the Privacy and Electronic Communications Directive (PECD) 'particularise and complement'[81] the DPD for the purpose (*inter alia*) of protecting the confidentiality of users' communications through publicly available networks and services. Among the matters regulated by the PECD are the surveillance, interception, storage and retention of users' communications and any related traffic and location data.[82]

The Telecoms package was amended in December 2009,[83] after extensive negotiations that one commentator has claimed were 'hi-jacked' by opponents of the further spread of graduated response regimes across the EU's Member States.[84] The amendments included changes to Article 1(3) of the Universal Service Directive, which now provides that measures taken by Member States regarding end-users' access to, or use of, the Internet "shall respect the fundamental rights and freedoms of natural persons, including in relation to privacy and due process."[85] A new paragraph added to Article 1 of the Framework Directive echoes this, but further stipulates that where fundamental rights are engaged by such measures, the latter can only be imposed if appropriate, proportionate, necessary within a democratic society, and subject to adequate procedural safeguards including effective judicial protection and due process. Accordingly, such measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure must be guaranteed, including the right of the person concerned to be heard; and the right to effective and timely judicial review shall also be guaranteed.[86] These amendments represent a dilution of two earlier proposals – referred to throughout the blogosphere as 'Amendment 166/Article 32(a)' to the Universal Service Directive and 'Amendment 138/Article 8.4(g)' to the Framework Directive – that were originally promoted by large majorities in the European

[81] Article 1(2) PECD.
[82]Traffic data relate to e.g. the routing, duration, time, format and volume of electronic communications. Location data give the geographic position of a user's terminal equipment.
[83] See Directive 2009/140/EC (amending the Framework, Access and Authorisation Directives) [2009] OJ L337 and Directive 2009/136/EC (amending the Universal Service and E-Privacy Directives) [2009] OJ L337.
[84] Francesco Rizzuto, "European Union Telecommunications Law Reform and Combating Online Non-Commercial Infringements of Copyright" (2011) *Computer and Telecommunications Law Review* 75.
[85] Article 1(1) Directive 2009/136/EC
[86] Article 1.1(b), Directive 2009/140/EC (inserting a new Article 1.3(a) into the Framework Directive). See also Recital 4 (recognising that the Internet is essential for education and for the practical exercise of freedom of expression and access to information).

Parliament. Amendment 138 in particular would have required disconnection from the Internet to be authorised by a court except where public security was threatened:[87] its objective was to ensure that Member States would be prohibited from introducing 'three strikes' regimes without judicial oversight. By contrast, the prior 'fair and impartial procedure' and 'judicial review' now referred to in Article 1.3(a) of the Framework Directive seem only to guarantee a court hearing on appeal from an initial ruling (which must be 'fair and impartial' but could be non-judicial) to disconnect.[88]

At the international and regional levels, then, efforts had been under way since 2008 to advance policies that – formally or informally – would have put IAPs' informational and technical resources at the service of copyright owners so that Internet users' activities could be more effectively monitored and infringing activities more effectively curtailed. These efforts had been contested by broad coalitions of Internet businesses and civil society groups on the ground that they would harm, rather than help, the digital economy while at the same time threatening the rights and freedoms of Internet users. It was against this backdrop that the UK Government's own policy to combat online copyright infringement, now expressed in the DEA, first took shape.

2.3 Background to sections 3-16 DEA

The first explicit commitment by the UK Government to enact legislation compelling IAPs to crack down on illegal file-sharing – apparently in response to energetic lobbying by the music industry[89] – was made with the publication in February 2008 of the *Creative Britain* report, setting out the New Labour Government's policy on the creative industries. However, what the Government actually announced here was a strategy of encouraging right-holders and IAPs to work together to agree an approach to curbing illegal file-sharing, while insisting that it would not hesitate to legislate in this area *if* no common approach could be agreed. While maintaining a robust system of copyright protection, it would also encourage content providers and network operators to work together to develop "new business models which recognise changes in technology – and their democratisation of content – yet capture the value provided by content producers and distributors."[90] The Government's view seemed to be that illegal file-sharing was a symptom, not simply of a widespread lack of respect for IPRs and IAPs' blinkered concern with growing their share of the broadband market, but also of content providers' failure to respond to consumer perceptions that content should (and could) be made available online in more appropriately priced and convenient formats than those currently available. It made business sense, the Government hinted, for content providers to develop new products and services to offset the decline in their traditional revenues, and equally for network operators to diversify beyond the provision of access and pipes into the distribution of legitimate content under licence from right-holders. Hence "the integration of anti-piracy

[87] See http://www.laquadrature.net/wiki/Telecoms_Package_Plenary_Amendments#Amendment_138_.2B.2B.2B.

[88] For critical commentary, see Monica Horten, "Telecoms Package: The Verdict" (http://www.iptegrity.com 13 November 2009)

[89] John Naughton, "A clampdown is music to the record industry's ears" The Observer, 17 February 2008 (available at: http://www.guardian.co.uk/media/2008/feb/17/3/print).

[90] *Creative Britain* p.50

measures into a wider collaboration between content and network providers could create a healthier digital environment which would benefit consumers and creators."[91]

In July 2008, a Memorandum of Understanding on an Approach to Reduce Unlawful File-sharing (MoU) was agreed between key 'stakeholders' from the ISP industry, the content industries, OFCOM and the Government. In an obvious attempt to take forward the 'wider collaboration' sought by the Government, the MoU committed signatories to cooperate, not only in devising and operationalising a process for curbing mass file-sharing and joining a group convened by OFCOM "to explore effective mechanisms to deal with repeat infringers,"[92] but also in educating consumers about the damage done to the creative industries by infringing activity (thereby changing public attitudes to copyright) and organising legal access to content in a variety of new formats (thereby routing consumer demand for unlawful file-sharing services towards attractive lawful alternatives). Mechanisms to be considered by the group would include "technical measures such as traffic management or filtering and marking of content"[93] that would require intervention by ISPs, as well as actions right-holders might take against serious infringers. The group would ultimately produce codes of practice governing the deployment of these mechanisms. All codes would require the approval of OFCOM: this was designed to ensure that they accorded with the principles governing all of OFCOM's regulatory activities, and hence that the actions required by the codes would be non-discriminatory, objectively justifiable, proportionate, transparent, strike an appropriate balance between the interests of right-holders and IAPs and comply with relevant provisions of EU and domestic law.

However, many smaller IAPs were not party to the MoU, generating concerns that non-cooperative IAPs would attract subscribers away from signatories and thereby precipitate the collapse of the agreement.[94] The Government's next step (in July 2008) was to propose a different kind of co-regulatory regime than that initially envisaged, for dealing with the specific issue of unlawful P2P file-sharing.[95] It proposed that IAPs and right-holders would – with the Government's encouragement – cooperate along the lines set out in the MoU, in particular by producing codes of practice setting out the kinds of actions that IAPs would be expected to take against alleged online infringers. However these codes would be accompanied by a duty on all IAPs, enshrined in legislation, to have an effective policy in place for dealing with cases of alleged unlawful file-sharing, and to act to implement that policy where it could be demonstrated that an individual subscriber was infringing copyright.[96] That duty – which "would be designed to apply only to unlawful file-sharing over P2P networks"[97] – could be discharged by demonstrating compliance with the codes, but IAPs not party to the self-regulatory arrangement would remain bound by the underlying requirement.[98]

[91] Ibid.
[92] BERR, "Consultation Document on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing" (July 2008), (Annex D) p.47.
[93] Ibid. p.48
[94] Ibid, paras. 6.2, 8.6.
[95] Ibid paras. 8.1-8.12.
[96] Ibid para 8.9.
[97] Ibid.
[98] Ibid, para. 8.10.

By January 2009 it was apparent to the Government that this approach would not work as initially conceived either: the proposed IAP obligation was considered too vague, and the overall approach not guaranteed fairly to represent the interests of all stakeholders, including the smaller IAPs and consumers.[99] What then emerged was yet another version of the co-regulatory approach, under which the regime governing online copyright infringement would comprise a combination of legislative provisions clearly defining the kinds of actions IAPs would be obliged to take against alleged infringers, and industry codes dealing with the implementation of these obligations. IAPs would be legally required to take two kinds of action when specific instances of infringing activity by their subscribers (identified at this point only via their IP addresses) were reported to them by right-holders.[100] The first obligation would be to notify the alleged infringer of the reported infringement. The second would be to keep records of the number of notifications linked to each subscriber, compile lists of subscribers with multiple notifications (anonymised to ensure compliance with data protection legislation), and make these lists available to the relevant right-holders on request. Right-holders could use the lists to single out subscribers who appeared to be repeat infringers and apply for a court order to obtain the names and addresses of those on the lists. This in turn would pave the way for right-holders to "take targeted legal action against those who appear to be responsible for the most damage to the [creative industries]."[101]

The Government insisted that what it called the 'practical details' of the two proposed obligations – such as what standard of evidence should be required to support a notification of infringement, how many notifications would justify inclusion in a list of repeat infringers, and what kind of appeal mechanism should be available to subscribers who believed they were wrongly accused of infringement – should not be set out in legislation but rather in an industry code of practice.[102] It clearly retained the hope that an 'industry body' (*not* a new government regulator) bringing together content providers and IAPs would emerge to draft a code of practice for OFCOM to approve,[103] failing which OFCOM would have a backstop power to create its own code. Hence during the first half of 2009, the Government sought views on the potential for the creation of such a 'Digital Rights Agency', and – as it had when the MoU was concluded – it still envisaged this as having a number of possible roles in relation to the online use of copyright material, not limited to that of devising a process to deal with file-sharing.[104] By November 2009 no such agency had materialised, and legislation had been drafted to prepare the ground for the two obligations outlined above (as well as other related obligations to be discussed

[99] BIS, "Government's Response to the Consultation Document on Legislative Options to Address Illicit P2P File-Sharing" (June 2009), p.4.
[100] Ibid and *Digital Britain: Interim Report* (Cm 7548) (January 2009), Section 3.2; *Digital Britain: Final Report* pp.111-112, paras. 24-31.
[101] BIS/DCMS, "Copyright: Factsheet" (November 2009).
[102] BIS, Government's Response to the consultation document on legislative options to address illicit P2P file-sharing" (June 2009) p.5.
[103] *Digital Britain: Interim Report* p. 42.
[104] DCMS/BERR/DBIS, "Copyright in a Digital World: What Role for a Digital Rights Agency" (March 13, 2009). The roles envisaged for the agency here included raising awareness of the importance of copyright to the creative industries, providing consumers with information about online sources of legal content, and "marriage brokering" between content providers and ISPs.

below). Having been introduced in November 2009, the Digital Economy Bill had passed the Lords by mid-March 2010; by 8 April it had received Royal Assent after being rushed through the Commons by means of the 'wash-up' procedure – normally only used to ensure that uncontroversial legislation can be passed quickly before a Parliament is dissolved – ahead of the April 12 dissolution of Parliament in advance of the 6 May General Election. Shortly thereafter, OFCOM issued its own draft Initial Obligations Code for consultation.

Almost immediately, BT and TalkTalk sought judicial review of the DEA's online copyright infringement provisions, and of the draft Statutory Instrument setting out how the costs associated with the initial obligations were to be apportioned. The main ground of challenge was that sections 3-18 DEA should themselves have been notified in draft to the EU Commission as a regime of technical regulations/rules on information society services within the meaning of the Technical Standards Directive, and that since they were not so notified the provisions were unenforceable. The claimants also argued that the contested provisions were incompatible with the E-Commerce Directive, the Privacy and Electronic Communications Directive, and the Authorisation Directive; and that they were disproportionate in their impact on IAPs, on consumers, and on subscribers (such as public libraries) who also provide Internet access to end-users. In April 2011 the High Court ruled against the claimants on all grounds except one (the compatibility of the cost-sharing Order with the Authorisation Directive).[105] The Court of Appeal is due to hear an appeal against this ruling early in 2012.

3 THE "INITIAL OBLIGATIONS"

3.1 The Legislation

Sections 3-16 amend the Communications Act 2003 (c.21) (hereinafter CA) by the insertion into that Act of new sections 124A-N. Sections 124A-B CA outline two "initial" obligations that may be imposed on any ISP whose service consists "entirely or mainly of the provision of access to the internet" and includes the allocation of IP addresses to subscribers (i.e., any IAP).[106] The first is to send notifications to subscribers following receipt of reports – "copyright infringement reports" (CIRs) – from copyright owners that these subscribers have been engaging in copyright-infringing activity.[107] The second is to maintain anonymised "copyright infringement lists" (CILs) of subscribers who appear to be persistent infringers and make these available to copyright owners on request.[108] "Subscriber" is defined as a person who receives an internet access service under an agreement with the service provider, but

[105] *British Telecom plc and Another, R v Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin) (20 April 2011).
[106] Section 124N CA.
[107] Section 124A CA.
[108] Section 124B CA. Section 124B(2)(b) provides that these lists must not enable any subscriber to be identified. To serve their intended purpose, however, the lists will have to be able to distinguish listed subscribers from each other in terms of the number of CIRs relating to each; and this will involve the use of unique identifiers of some kind.

not as a communications provider.[109] Under new section 124A(1) CA, a right-holder may issue a CIR if it appears to them that a subscriber has (a) infringed their copyright by means of an internet access service or (b) has allowed another person to use the service, and that other person has infringed the right-holder's copyright. The question here, then, is not whether the subscriber has actually given permission to another person to use his/her service, much less that s/he has actually given permission to another to use it for infringing purposes: the issue is simply whether it *appears to the right-holder* that the subscriber has allowed another person to use their service, and that person has infringed the right-holder's copyright.

Here the de-centred (or 'networked') regulatory strategy characteristic of the DEA – and the rich mix of regulatory agents and instruments already noted in Part 2.1 above – is very clearly in evidence. As section 124A(1) shows, subscribers are to be the focus of the IAP's notifying activities, regardless of whether they themselves have infringed or knew of others' infringing activities. This in turn seems calculated to mobilise householders in particular to police all Internet use occurring within their homes. The same would seem to apply to employers in relation to their staff, but also to libraries, educational institutions and other providers of open access wi-fi facilities in relation to all the many (and mostly anonymous) users who make use of these facilities. The DEA will incentivise these private parties to, for example, encrypt their services so that only particular individuals will be able to use them (something at odds with very concept of open access and indeed the spirit of the *Digital Britain* report);[110] and/or to block or filter content themselves.[111] The notification process envisaged by

[109] Section 124N CA A communications provider is defined in section 405 CA as a person who provides an electronic communications network or service. Hence the DEA presupposes a distinction between upstream and downstream provision of internet access. However, not all purchasers of broadband services who then 'provide' Internet access to end-users – from householders running unsecured wi-fi networks in their homes to Internet cafés charging by the hour for access through dedicated terminals – will necessarily be treated as 'communications providers' under the DEA: it would appear from the guidance issued by the Government and OFCOM that this should depend on the terms and conditions on which they both receive the upstream service and provide the downstream service. OFCOM has taken the view that where, for example, a hotel purchases a service from a broadband provider in order to be able to provide Internet access to its guests in their rooms, it should be regarded as a communications provider rather than a subscriber; however, it might also itself be an Internet access provider within the meaning of the DEA if its guests could be regarded as subscribers and the service included allocating IP addresses to them. A person or undertaking that receives an internet access service for its own purposes is in OFCOM's view a subscriber, even if it also makes access available to third parties (see OFCOM, "Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code" (28 May 2010), paras. 3.19-3.31; see also BIS/DCMS, "Online Infringement of Copyright: Libraries, Universities and Wi-Fi Providers" (February 2010). For a compelling diagnosis of the uncertainties likely to be generated in practice by the subscriber/communications provider distinction, see Nick Cusack, "Is the Digital Economy Act 2010 the Most Effective and Proportionate Way to Reduce Online Piracy?" (2011) 33(9) *European Intellectual Property Review* 559-564.

[110] Ibid, . p.561.

[111] The Government and OFCOM are actively encouraging such private initiatives by joining with several major companies in the media, communications and creative sectors in sponsoring a website offering advice to computer users on how to use the Internet "confidently, safely and securely" (www.getsafeonline.org). The website lists three companies – Cybersitter, NetNanny, and Cyberpatrol – that provide filters and blocking software. Since notifications issued to subscribers are required under section 124A(6)(h) CA to include "advice … about steps that a subscriber can take to protect an internet access service from unauthorised use" it is likely (whether or not the initial obligations code so requires) that notifications will direct subscribers to the products of such companies.

the Act will also be a vehicle for educating subscribers about the importance of respecting copyright, and prompting them to seek out lawful sources of copyright content online.[112]

New sections 124C-D CA (inserted by sections 5-6 DEA) oblige OFCOM to approve or make an "initial obligations code," which once in force would bring the two initial IAP obligations into effect, define them in detail and institute mechanisms for their implementation. New sections 124C-E together set out procedural and substantive criteria governing the making or approval of this code. Section124E (inserted by section 7 DEA) sets out what the code must contain, including *inter alia* details of the procedures that right-holders and IAPs must follow in relation to the two initial obligations – in particular concerning the standard that evidence must meet if it is to justify a CIR, the format and content of the notification letters sent by IAPs, and the means of determining the subscribers ('relevant subscribers') eligible for inclusion in the CILs that ISPs are obliged under section 124B to maintain.[113] Section 124E also stipulates that the code must provide that OFCOM administer and enforce it,[114] and that it meet the requirements of new section 124K CA (inserted by section 13 DEA) concerning subscriber appeals. Under section 124K the code must confer on subscribers the right to appeal to a person who is independent of IAPs, right-holders and OFCOM;[115] there is no requirement that the code provide for a judicial hearing. As far as the initial obligations are concerned a subscriber appeal is an appeal by a subscriber, on grounds specified in the code, in relation to the making of a CIR about a subscriber, its notification to the subscriber, the inclusion of a subscriber in a CIL, or "any other act or omission in relation to an initial obligation or an initial obligations code."[116] The code must include as possible grounds for appeal that a CIR is flawed in that it does not relate to an act which amounts to a copyright infringement, and/or that an apparently infringing act was incorrectly attributed to the subscriber's account (the burden of showing that a CIR is irreproachable in both respects rests on the respondent[117]); and that the right-holder or IAP has contravened the code or an obligation regulated by the code. The code must also provide that a subscriber appeal must succeed in respect of a CIR where the subscriber shows that the act described in the CIR was not carried out by the subscriber and that the subscriber took reasonable steps to prevent other persons using their account to infringe copyright.[118]

[112] See section 124A(6) CA (setting out what a notification to a subscriber must include).
[113] These will be subscribers who have been the subject of a number of CIRs exceeding the threshold set in the initial obligations code (section 124B(3) CA) – i.e. repeat infringers.
[114] OFCOM's enforcement role includes the power to impose penalties on right-holders and ISPs for contravening an initial or technical obligation (sections 124L, CA; 124E(8)(a) and 124J(3)(a) CA), the power to require right-holders to indemnify IAPs for any loss occurring as a result of their failure to comply with the statutory provisions or the codes (sections 124E(8)(b) CA and 124J(3)(b) CA), and the power to resolve disputes between copyright owners and IAPs concerning acts or omissions in relation to the Codes (sections 124J(2))(a) and (4) CA; section 124E(7)(a) and (9) CA).
[115] Section 124K(2)(c) CA.
[116] Section 124N CA. The definition of 'subscriber appeal' in relation to a technical obligations code is different: see n 158 below below.
[117] Section 124K(6) CA
[118] Section 124K(6) CA.

3.2 The Initial Obligations Code

As noted already, the Labour Government's hope throughout the process of devising its programme of action on online copyright infringement had been that 'industry' would be able to devise a code for OFCOM to approve. This hope was reiterated in January 2010, when the Government acknowledged that it would be the code, not the primary legislation, that would effectively define the two initial obligations, the rationale being that "[t]his is a fast changing area of technology and consumer behaviour and the processes behind the obligations need to be flexible and adaptable if the obligations are to remain proportionate and effective."[119] In the end, OFCOM itself drafted an Initial Obligations Code,[120] and it bore out the Government's prediction, adding much detail to the vague picture yielded by the legislation of how the notification/listing system would operate in practice. Progress on finalising this Code was then delayed by a number of unforeseen developments – notably the High Court's ruling on British Telecom's legal challenge to sections 3-18 DEA (hereinafter *British Telecom*), which necessitated some changes to the May 2010 draft, in particular as regards cost-sharing. At the time of writing, the DCMS is reconsidering OFCOM's finalised text in the light of comments from the Regulatory Policy Committee.

The most noteworthy sections of the 2010 draft specify the following:

- The IAPs that will be subject to the two initial obligations. Only those IAPs providing a fixed Internet access service to more than 400,000 subscribers (currently seven UK IAPs) will qualify in the first instance. However OFCOM proposes to keep the qualification criteria under review, and if the number of potential CIRs made by right-holders in relation to non-qualifying IAPs rises significantly, to assume that this reflects migration by infringers to these other providers and alter the criteria to include them.
- The right-holders that will be able to take advantage of the two initial obligations. Only those that have sent estimates in advance to qualifying IAPs of the number of CIRs they intend to issue in a given period (so that IAPs can plan ahead and budget for the extra burden that processing these will impose on them), and have met their share of the costs of the notification/listing regime (specified in an order made by the Secretary of State under section 124M, considered below), will qualify.

[119] BIS/DCMS, "Online Infringement of Copyright: Outline of Initial Obligations Code" (January 2010). While the decision not to specify the details of the new regime in primary legislation has been a major focus of public criticism of the DEA, it assisted the Government in facing down the IAPs' challenge to the legality of sections 3-16. British Telecom and TalkTalk cited as one of their grounds of challenge that the initial obligations provisions should have been notified in draft to the EU Commission as a regime of technical regulations/rules on information society services within the meaning of the TSD, and that since they were not so notified they were unenforceable. However Parker J. ruled that only measures that by themselves have legal effect for individuals – because binding on, and sufficiently precise and specific to be enforceable against, individuals – need to be notified under the TSD; and that since the DEA's initial obligations provisions have no such effect in isolation from the Code "which gives [them] legal life and real content" (*British Telecom* para. 88) they – as distinct from the Code – were not notifiable.

[120] OFCOM, "Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code" (28 May 2010).

- The information that will have to be contained in CIRs. This includes the filenames of allegedly infringing files; relevant IP addresses, port numbers, website addresses and protocols; and details of the exact date and time of the alleged infringement.
- The notification process. The Code provides for this to involve a series of three notifications to apparently infringing subscribers, depending on their behaviour over time. The first will be sent after receipt by the IAP of the first CIR relating to that subscriber. The second will be sent after the first CIR relating to the same subscriber (though not necessarily from the same right-holder) to be received between one and six months from the date of the first notification. The third will be sent after the first CIR relating to the same subscriber to be received one month or later from the date of the second notification – unless this CIR is received more than 12 months after the first CIR. The Code's provisions regarding the content of these notifications largely reflect the requirements of new section 124A(6) and (7) CA.
- The process of compiling copyright infringement lists. Qualifying IAPs will be required to keep a database of all subscribers receiving a third notification within the previous 12 months. The criteria for determining the 'relevant subscribers' who may be included in a CIL provided by an IAP provides to a copyright owner are (a) whether the subscriber has been included in the database, and (b) whether that owner has sent at least one CIR relating to that subscriber within the previous 12 months. Each list will only contain information relating to CIRs sent by the requesting right-holder.
- Provision for subscriber appeals. The DEA requires OFCOM to establish an independent appeals body to determine subscriber appeals. The draft Code sets out this body's principal functions and the framework of rules within which it will be required to operate. Most of these rules mirror new section 124K CA, although the Code requires in addition, *inter alia*, that the appeals body protect the anonymity of subscribers in the appeals process. Once established, that body will institute detailed procedures for the determination of subscriber appeals in accordance with the Code. The Code envisages that only in exceptional circumstances, where the appeals body considers it appropriate, will oral submissions be accepted or oral hearings held in determining a subscriber appeal.

At this point it is worth emphasising once again that although the initial obligations regime will mobilise IAPs to engage in a 'graduated response' to allegations by right-holders of infringements by subscribers, at no point will the response involve their administering sanctions: to this extent, the initial obligations regime is not analogous to the more draconian French regime – which is a true 'three strikes' regime.[121] Unless and until the DEA's technical obligations are brought into effect, a graduated response *à l'Anglaise* can lead only to the sending of anonymised lists of apparently serial infringers to right-holders, who must then seek court orders to obtain the personal details of these individuals if they wish to take the further step of issuing infringement proceedings against them. Parker J. pointed out in *British Telecom* that

[121] Cf. Eldar Haber, "The French Revolution 2.0: Copyright and the Three Strikes Policy [3SP]" (2010) 2(2) *Harvard Journal of Sports & Entertainment Law* 297-339 (suggesting that a single '3SP' is emerging globally on the model of the French *Création et Internet* legislation).

this system is "more efficient, focussed and fair"[122] than the pre-DEA arrangements, which have effectively incentivised right-holders to use the blunt (and intimidating) instrument of legal action indiscriminately against everyone suspected of any infringement whatsoever.[123] Nonetheless, the picture of the reporting, notification and listing processes that emerges from the draft Code will not entirely reassure those who are concerned about the DEA's implications for civil liberties, and Internet freedom in particular. On the one hand, OFCOM is clearly concerned to ensure that these processes produce accurate CIRs, notifications and CILs, so that "where allegations are made against subscribers they are based upon credible evidence, gathered in a robust manner."[124] The Code will require right-holders to provide annual quality assurance reports to OFCOM on their processes for linking IP addresses with infringing activity, so that the regulator can be sure that these are robust and yield accurate results. It will also require IAPs to have in place effective technical systems to link IP addresses with particular subscribers, so that the regulator can be sure that these reliably identify the subscribers that ought to receive notifications. Yet the more accurate these processes and systems, the more potent the capacity of right-holders and IAPs to track individuals' Internet usage: paradoxically, systems designed to eliminate one source of grievance for individuals (false accusations of copyright infringement) necessarily give rise to another (that every move they make online will be subject to surveillance and traceable back to them). This in turn raises issues about the compatibility of the initial obligations regime with the freedom and confidentiality of Internet users' communications, matters heavily regulated by EU law.

3.3 The Initial Obligations Regime and EU Law

Article 15 of the E-Commerce Directive (ECD) – preventing Member States from imposing general obligations on ISPs to monitor the content they transmit or store, or actively to look for evidence of unlawful usage of their facilities – is arguably justified in part by the concern that these private actors should have no incentive to censor their users' communications. In *British Telecom*, Parker J. was disinclined to hold that the legislative design of the initial obligations regime contradicted Article 15. Requiring IAPs to notify, and maintain lists of, allegedly infringing subscribers would not, in Parker J.'s view, amount to obligations on them to monitor the information they transmitted, or to examine all their subscribers' usage with a view to finding infringing communications, but only to identify particular alleged wrongdoers in response to reports from right-holders who had taken it upon themselves to monitor the activities of Internet users in general. However this analytical separation of monitoring from identification seems artificial in relation to the regulatory strategy underlying the DEA. As noted in Part 2 above, that strategy consists precisely in breaking down a regulatory function – that of curtailing online copyright infringement – into a number of constituent elements, and distributing these amongst a variety of actors perceived as having the capacity to contribute to the function's discharge. In effect, the DEA's initial obligations regime makes the IAP an agent of those right-holders who are *de facto* engaged in general monitoring of the information they (IAPs) transmit, and actively seeking circumstances indicating illegal activity.

[122] *British Telecom*, para. 228.
[123] See e.g. *MediaCAT v Adam* [2011] EWPCC 6.
[124] OFCOM, 'Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code' para 1.3

Even if this monitoring involves no formal conflict with Article 15 ECD, a further question arises concerning its compatibility with the protection for Internet users' privacy that EU law requires. The production of CIRs by copyright owners, first of all, will involve finding and recording dynamic IP addresses – activities which will arguably render them 'controllers' of the 'processing' of 'personal data' within the terms of EU data protection law.[125] Moreover the material identified as linked with these addresses could fall into one or more of the special categories of personal data (concerning e.g. the political opinions of the user) listed in Article 8 of the Data Protection Directive (DPD). However in *British Telecom*, Parker J. stressed that the DPD did not prevent Member States from allowing the processing of personal data – whether it falls within or outside the sensitive categories – where "necessary for the establishment, exercise or defence of legal claims";[126] and that it was precisely the purpose of the contested provisions to facilitate copyright owners in establishing and exercising their legal claims against infringers. Further, Parker J. accepted that IAP activities of notifying subscribers and compiling CILs, though clearly also involving the processing of personal data within the meaning of the DPD, were authorised as "necessary for compliance with … legal obligation[s]" to which IAPs will be subject once the Code is in force.[127]

The processing of personal data "in connection with the provision of publicly available electronic communications services in public communications networks in the Community" is however subject to additional regulation under the Privacy and Electronic Communications Directive (PECD).[128] The data processed by both copyright owners and IAPs under the initial obligations regime will include subscribers' 'traffic data', and the DEA's endorsement of the tracking of user communications by these actors *prima facie* contravenes the obligation on Member States under Article 5 PECD to "ensure the confidentiality of [Internet users'] communications and the related traffic data." Moreover, the Act's imposition of obligations on IAPs to make CILs ostensibly contravenes the requirement imposed on ISPs under Article 6 PECD that traffic data be "erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication."[129] However, both of these Articles are without prejudice to Article 15(1) PECD, which allows Member States to adopt legislative measures restricting the obligation to respect the confidentiality of users' communications and related traffic data. The compatibility of the reporting and listing activities envisaged by the DEA with the PECD therefore depends on whether these activities come within the scope of a derogation that in turn is covered by Article 15(1).

[125] For an analysis of EU law relating to the processing of IP addresses with a view to detecting file-sharers, see Fanny Coudert and Evi Werkers, "In the aftermath of the *Promusicae* case: how to strike the balance?" (2010) 18(1) *I.J.L. & I.T.* 50. On the status of IP addresses as personal data, see Patrick Lundevall-Unger and Tommy Tranvik, "IP Addresses – Just a Number?" (2011) 19(1) *I..J.L. & I.T.* 53-73. The CJEU has recently confirmed that IP addresses are personal data: see *Scarlet v. SABAM* (Case C-70/10) (24 November 2011), para. 51.
[126] Article 8(2)(e) DPD.
[127] See DPA 1998 Sch .2 para. 3, which mirrors Article 7(c) DPD.
[128] Article 3(1) PECD.
[129] This Article permits the storage and processing of traffic data for certain purposes (e.g. for the purpose of billing a subscriber), but none of these purposes applies to IAP activities under the DEA.

Prior to the enactment of the DEA, the ECJ had already ruled in *Promusicae v Telefónica* that Article 15(1) allowed PECD obligations to be restricted not only in the circumstances specifically mentioned there (i.e. to safeguard public security and national defence, and for the purposes of investigating criminal offences and unauthorised use of the electronic communications system), but also in situations "that may give rise to civil proceedings."[130] The Court arrived at this surprisingly broad interpretation of Article 15(1)[131] by emphasising the express reference contained in that paragraph to Article 13(1) of the Data Protection Directive. This mentions further purposes for which Member States may restrict the right to privacy in respect of the processing of personal data, including where the restriction is necessary "for the protection of the rights and freedoms of others." The Court concluded that, read in relation to Article 13(1) DPD, Article 15(1) PECD had to be interpreted "as expressing the Community legislature's intention not to exclude from [its] scope the protection of the right to [intellectual] property *or* situations in which authors seek to obtain that protection in civil proceedings."[132] The question posed by the referring court was then answered by the Court's ruling that although EU law does not require Member States to implement in their national laws an obligation to disclose personal data in the context of civil proceedings in order to ensure the effective protection of copyright, it does not preclude this either. What EU law does require, the Court went on, is that Member States transposing the relevant Directives in this area interpret them in a way "that allows a fair balance to be struck between the various fundamental rights protected by the Community legal order;" and that "when implementing the measures transposing those directives, the … courts of the Member States … not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality."[133] The Court offered no guidance as to how either legislatures or courts might fulfil these duties.

In *British Telecom*, Parker J. seemed to broaden the reach of *Promusicae* beyond the decision actually taken on the reference, concluding that the DEA's initial obligations regime – which will involve the processing of personal data *outside* the context of civil proceedings – is justified by Article 15(1) PECD *simply* because it is intended to promote the protection of copyright.[134] Further, he failed to do what *Promusicae* required him to do: namely, first analyse whether the contested provisions of the DEA *struck a fair balance* between the fundamental rights in issue, and then ensure that his

[130] *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] 2 CMLR 17, para. 52. Promusicae, a Spanish organisation of right-holders in sound recordings, had applied to a Spanish court for the equivalent of a *Norwich Pharmacal* order, requiring Telefónica, a Spanish IAP, to disclose the identities and physical addresses of subscribers who Promusicae claimed were infringing their copyrights, so that Promusicae could bring civil proceedings against these alleged infringers. The order was granted by the national court, but Telefónica appealed against that order, contending that there was no authority in the court under EU law to order the communication of the data sought in the context of civil proceedings or as a preliminary measure relating to civil proceedings. The national court referred that question to the ECJ.

[131] Compare the Advocate General's Opinion in *Promusicae* [2007] ECJ C-275/06 (indicating that all the grounds for derogation in Article 15 PECD concerned public security, and implying that an extension of these grounds to cover civil disputes would stretch the Directive's language too far).

[132] *Promusicae v Telefónica* (ECJ) para. 53 (emphasis added).

[133] Ibid. paras. 68 and 70.

[134] *British Telecom* paras. 165-6.

own interpretation of the relevant Directives did not conflict with those rights, or with the principle of proportionality. Parker J. did not analyse the implications for privacy of the contested provisions, although the right to privacy is clearly a fundamental right protected by the Community legal order. Meanwhile, he seemed to accept the Secretary of State's view that copyright was also such a right, although this is controversial.[135] The effect of the contested provisions on freedom of expression was noted – in particular, Parker J. accepted that there was some risk that the private policing by subscribers of the use of their Internet connections by others would have a chilling effect on legitimate Internet use – but pending the coming into effect of the initial obligations, it was in his view premature to conclude that any social costs thereby incurred would greatly outweigh the social benefits in terms of enhanced copyright protection.[136] As to proportionality more generally, Parker J. adopted a highly deferential approach to the balance struck by Parliament in the short time that was available to it to consider the Digital Economy Bill. The contested provisions, he said, addressed "a major problem of social and economic policy, where important and conflicting interests [those of the nation and the copyright industries in curbing the economic damage caused by unlawful online activity, those of IAPs in minimising their responsibility for the material passing through their conduits, and those of Internet users in enjoying untrammeled access to online content] are in play."[137] This was an area firmly within the province of the legislative branch, not least because its complexity exposed the limits of the adjudicative process:

> Parliament struck the challenged balance after a lengthy process of consultation with all interested parties, which took account of the representations made by those parties, and after a voluntary, non-legislative scheme was tried out. That process is likely to have provided the decision maker with an insight and capacity that the court is unlikely to enjoy.[138]

The contested provisions, Parker J. concluded, pursued the legitimate objective of protecting the 'fundamental right' to (intellectual) property, were necessary (because the hoped-for co-regulatory solution had failed to materialise) and had not been shown to be disproportionate – "in other words, that the legislator unlawfully failed to balance the relevant interests at stake."[139] As to the latter, it sufficed as far as Parker J. was concerned that the legislator had *taken into account* all the relevant interests: the

[135] Ibid para. 215. The only support offered for that proposition was Article 17(1) of the Charter of Fundamental Rights of the EU, which declares that "everyone has the right to own … his or her lawfully acquired possessions." Article 17(1) does not mention intellectual property; Article 17(2) states only that "intellectual property shall be protected", a form of words not apt to suggest that intellectual property is a fundamental right on a par with other rights specified in the Charter (see further Christophe Geiger, "Intellectual Property Shall be Protected!? Article 17 (2) of the Charter of Fundamental Rights of the European Union: a Mysterious Provision with an Unclear Scope" (2009) 31(3) EIPR 113). In its recent decision in *Scarlet v. SABAM* (n 124), the CJEU avoided stating unequivocally that intellectual property is a fundamental right in this sense (see paras. 43-44), but offered no clear characterisation of the place intellectual property occupies in the Charter's overall scheme. For a detailed and comprehensive examination of the current legal status of the Charter (though it also lacks an adequate analysis of the status of Article 17), see Kieron Beal and Tom Hickman, "*Beano* No More: The EU Charter of Rights after Lisbon" [2011] *Judicial Review* 113-141.
[136] *British Telecom* para. 240.
[137] Ibid, para 211.
[138] Ibid, para .212.
[139] Ibid, para. 243

fact that errors may have been made in *weighing* how the legislation would serve these interests was irrelevant. Hence voluminous expert evidence questioning the reliability of the estimates on the basis of which the DEA's anti-infringement strategy had been formulated – estimates of the impact of P2P file-sharing on the copyright industries, the likely impact of the new regime on the incidence of infringement, and the total social cost of the new regime – could be discounted, as it did not show that Parliament proceeded on the basis of irrational and unjustifiable assumptions.[140] It was enough that there were reasons for believing that the new regime "may well have [a] positive effect"[141] in curtailing online infringement.

This decision will have done nothing to convince critics of the DEA's online copyright infringement provisions of the legitimacy of the regulatory strategy embedded in it. Parker J.'s approach to the question of proportionality avoided any assessment of the substance of the legislative solution chosen to deal with the perceived problem of online copyright infringement, thereby revealing proportionality review to be somewhat toothless, in this area of policy at least.[142] The judgment eschewed any assessment of whether other equally (or more) effective solutions to the perceived problem might have been chosen that were less apt to endanger Internet users' privacy. It acknowledged the strategy's propensity to trigger activities that could threaten freedom of expression, but declared the threat inchoate pending the Act's full implementation. Finally, the ruling rests on the premise that the fundamental rights guaranteed by the European legal order, far from constituting bulwarks against the diffuse forms of private regulation that will be triggered by the DEA, can be interpreted as justifying such regulation.

It remains to be seen whether the Court of Appeal will find any challenges to this premise in the CJEU's recent ruling in *Scarlet v. SABAM*. Here the European Court held that IAPs cannot be ordered by national courts to filter all of their subscribers' electronic communications with a view to detecting and blocking files containing material that infringes copyright. Such an injunction, the Court unsurprisingly ruled, would require the IAP to carry out general monitoring in breach of Article 15 ECD. Yet the CJEU also insisted that the compatibility with EU law of measures designed to enable the more effective enforcement of copyrights depended more generally on the outcome of the balancing exercise required by *Promusicae*:

> [I]t follows from paragraph 68 of that judgment that, in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.[143]

[140] Ibid, para. 258.
[141] Ibid, para .233.
[142] See *British Telecom* para. 210 (where Parker J. referred approvingly to Lord Nicholls' proposition in *Wilson v. First County Trust Ltd. (No. 2)* [2003] UKHL 40 that "[t]he more the legislation concerns matters of broad social policy, the less ready will be a court to intervene") and para. 241. Tellingly, BT and TalkTalk have appealed every element of Parker J.'s ruling except this one, on the basis that their chances of success on this ground were always likely to be slim. For a critical assessment of the UK courts' approach to proportionality review in a range of contexts, see Tom Hickman, "The Substance and Structure of Proportionality" (2008) *Public Law* 694.
[143] *Scarlet v. SABAM* para. 45.

In the view of the Court, an injunction of the form sought by SABAM (a music copyright collecting society) would have failed to strike a fair balance between the applicants' copyrights on the one hand and the Charter rights of both the IAP and its customers on the other. The Court particularly noted the burdens the injunction would have imposed on the IAP's freedom to conduct its business pursuant to Article 16 of the Charter (the IAP would have been required to install a costly filtering/blocking system at its own expense), and on the rights of its customers to protection of their personal data pursuant to Article 8 (the system would have involved analysing activity linked to all of these customers' IP addresses), and to receive and impart information pursuant to Article 11 (the system could have led to the blocking of their lawful communications). Clearly, the reporting and notification processes mobilised by the DEA's initial obligations regime would be considerably less burdensome to the Charter rights and freedoms of IAPs and their customers than the injunction that SABAM sought to impose on the Belgian IAP, Scarlet. Nonetheless, the CJEU's ruling entails that the Court of Appeal must now review the DEA in a way that gives these burdens a greater weight than that accorded them by Parker J in the High Court.

Even if the Court of Appeal finds that the DEA's initial obligations regime achieves a fair balance of all the relevant rights, the *technical* obligations regime would, if implemented, involve measures more directly analogous to those considered in *Scarlet v. SABAM*, and considerably more difficult to justify as consistent with EU law. This regime is the focus of the next Part.

4 THE "TECHNICAL OBLIGATIONS"

As indicated in Part 2.3 above, active consideration was being given in the UK, from at least the period of the MoU negotiations in 2007-2008 to the possibility of devising codes of practice defining when IAPs could be expected to deploy technical measures against subscribers to prevent their networks from being used for copyright-infringing purposes. Yet until the middle of 2009, there was no hint that the Government would legislate to require IAPs to introduce these measures: its thinking seemed to be that imposing the notification and listing obligations would be enough to reduce the level of online infringement through a combination of warnings/education and facilitating the pursuit of serious infringers through the courts. However, by the middle of 2009 the Government was also proposing that OFCOM would be granted backstop powers to oblige IAPs to utilise technical measures against repeat infringers should these two obligations fail to reduce significantly the level of online infringement.[144] The final *Digital Britain* report, published in June 2009, indicated that legislation would specify what these measures might be, and that they would include blocking; bandwidth capping (capping the speed of a subscriber's Internet connection and/or capping the volume of data traffic which a subscriber could access); bandwidth shaping (limiting the speed of a subscriber's access to selected protocols/services and/or capping the volume of data to selected protocols/services); and content identification and filtering.[145]

[144] *Digital Britain: Final Report* pp.111-113
[145] Ibid, . p.111–112

However the report clearly stated that these powers should only be able to be used if the notification/listing regime did not succeed in significantly reducing the level of unlawful file-sharing: a 70% reduction was identified as the target. According to the report, if that regime had produced no significant impact after 6 months, OFCOM should begin to take steps to prepare for the introduction of technical measures. If there was still no significant impact after 12 months, technical measures would be introduced.[146] In June 2009, a consultation document was published inviting comments on these proposals.[147] Like *Digital Britain* itself, the document contained no reference to any possibility of temporarily or permanently disconnecting subscribers. However before the deadline for commenting on the consultation paper had been reached, the Government suddenly added two new proposals.[148] The first was that the Secretary of State be given powers to direct OFCOM to investigate whether technical measures should be required, and to direct OFCOM to require IAPs to impose these measures on subscribers. The second proposal was that disconnection of subscribers be added to the list of technical measures that OFCOM might require IAPs to impose on repeat infringers. Despite much public controversy, these revised proposals made their way into the Digital Economy Bill.

Under new section 124F CA (inserted by section 8 DEA as enacted), OFCOM must, as soon as an initial obligations Code is in force, prepare quarterly and annual progress reports regarding copyright infringement by subscribers to internet access services. Section 124F(5), in listing the matters that these reports must address, is clearly designed to ensure that they enable the Secretary of State to monitor trends in online copyright infringement, ascertain the effectiveness of the two initial obligations in curbing it, and decide in the light of this evidence whether an obligation to impose technical measures should be introduced. Significantly, the subsection also ensures that the reports may serve to inform the Secretary of State as to whether right-holders have performed their side of the bargain purportedly underlying the introduction of the notification/listing regime: the reports must also describe and assess the steps taken by right-holders to (re-)educate the public about copyright and to enable subscribers to obtain lawful access to copyright works. The implication seems to be that the Secretary of State may decline to introduce an obligation on IAPs to impose technical measures if the persistence of mass online copyright infringement can be attributed in part to the copyright industries' failure to contribute to a comprehensive solution to the problems that this causes for them. As was pointed out in one of the Government's notes on the Bill, "[t]he ultimate aim of the legislation is to shift people's behaviour from the unlawful to the legal,"[149] not merely to curb unlawful behaviour.

New section 124G CA (inserted by section 9 DEA) confers a power on the Secretary of State to direct OFCOM to assess whether IAPs should be obliged to take "technical measures" against "some or all relevant subscribers." A technical measure is defined very broadly as "a measure that (a) limits the speed or other capacity of the service

[146] Ibid p.112.
[147] BIS, "Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing" (June 2009).
[148] BIS, "Government Statement on the Proposed P2P File-Sharing Legislation" (25 August 2009).
[149] BIS/DCMS, "Online Infringement of Copyright: Outline of Initial Obligations Code" (January 2010)

provided to a subscriber; (b) prevents a subscriber from using the service to gain access to particular material, or limits such use; (c) suspends the service provided to a subscriber; or (d) limits the service provided to a subscriber in another way."[150] OFCOM may also be directed to take steps to prepare for the imposition of these technical obligations – such steps may under section 124G(5) include carrying out a consultation, assessing the likely efficacy of particular technical measures, and preparing a technical obligations code – and report back on the assessment and/or steps.[151] Nothing in section 124G as enacted requires the Secretary of State to await OFCOM's reports on the functioning of the notification/listing regime before issuing any of these directions.

New section 124H CA (inserted by section 10 DEA) gives the Secretary of State the power to impose a technical obligation on IAPs. Since "technical obligation" is defined as "an obligation … to take a technical measure" against subscribers,[152] this power would seem also to be a power to specify those measures. The power can only be used if the initial obligations code has already been in force for at least 12 months,[153] so although preparatory steps towards introducing technical measures can be taken before the impact of the notification/listing regime is known, such measures can only actually be introduced after that regime has been in operation for at least a year. Further, the requirement that OFCOM must first have assessed whether technical obligations should be imposed, together with the requirement that the Secretary of State have regard both to these assessments and to OFCOM's progress reports in deciding whether it is appropriate to impose technical obligations,[154] seems in keeping with the original governmental aim that these should only be imposed if the notification/listing regime fails to reduce the level of online copyright infringement significantly. On the other hand, the Secretary of State can also have regard to "any other matter that appears to him to be relevant"[155] in deciding whether to invoke the section 124H power, and the Government insisted during discussions of the Digital Economy Bill that the making of an assessment under section 124G was not intended to be a precondition for the power to make an order under section 124H:

> The Secretary of State needs to be able to make an order in the light of other considerations should the situation demand it. He needs to be able to take a broad view of the desirability of imposing a technical obligation. For example, the economic situation at the time might be something the Secretary of State might want to factor into the decision, or an assessment of potential unintended consequences of some measures on other policy areas.[156]

For any period in which technical obligations are in force, a code 'regulating' them must also be in force;[157] and new section 124I CA (inserted by section 11 DEA)

[150] See section 124G(3) CA.
[151] Section 124G(1) CA
[152] Section 124G(2) CA
[153] Section 124H(2) CA
[154] Section 124H(1) CA
[155] Ibid.
[156] Letter to the Chairman of the Delegated Powers and Regulatory Reform Committee from the Rt Hon Lord Mandelson, published as Appendix I to the Committee's Fourth Report of Sessions 2009-2010, HL Paper 41, 22 January 2010, para. 7.
[157] Section 124I(1) CA

requires that OFCOM make this code. The procedural and substantive criteria governing its making, set out in sections 124I-J, are similar in many respects to those applicable to the making of an initial obligations code: the most notable difference is that a technical obligations code must not only provide for a first subscriber appeal,[158] but confer a further right of appeal to the First-tier Tribunal.[159]

There is however a major difference between the legislative mechanisms underpinning the notification/listing and technical measures regimes. Whereas the two initial obligations have been set out in primary legislation – notwithstanding that much detail remains to be supplied by an OFCOM code – the potentially far more burdensome technical obligations will be defined entirely by Ministerial order together with an OFCOM code. Beyond stating that the Secretary of State's order may specify "the criteria for taking the technical measure concerned against a subscriber [and] the steps to be taken as part of the measure and when they are to be taken"[160] section 124H offers no guidance as to what form a technical obligations regime would take; and section 124G defines 'technical measures' in the vaguest possible terms. In specifying the technical obligations to be imposed on IAPs, any order under section 124H would also specify the technical measures to be imposed on "some or all relevant subscribers." It is clear that relevant subscribers will be (alleged) repeat infringers (subscribers eligible for inclusion in a copyright infringement list because linked with a sufficient number of CIRs); but it is not clear what would justify singling out 'some' of these for technical measures. As noted above, a technical measure could "suspend" a subscriber's access to the Internet – and it is not entirely clear that this implies only temporary disconnection – while the catch-all provision enabling measures to be imposed that "limit the service provided to a subscriber in any other way" is exceedingly open-ended.

Lord Mandelson, the Minister responsible for initiating the Digital Economy Bill, defended this 'skeletal' approach to the definition of the Secretary of State's and OFCOM's powers on the basis that technical matters, and details requiring adaptation and refinement over time, should not be included in primary legislation. However it has been argued by the Act's many critics that the drafters have represented as mere technicalities or details matters which are in fact crucial to the operation of the envisaged copyright enforcement regime; and that failure to specify these matters in primary legislation has made it impossible to judge whether the new mechanisms it anticipates for curbing copyright infringement will be necessary or proportionate in relation to the legislation's aim.[161] What is certain, however, is that both the Secretary of State and OFCOM will now be obliged to have regard to the CJEU's judgment in *Scarlet v. SABAM* (see 3.3 above) in making an order under section 124H and a code under section 124I. Both may be tempted to read that judgment narrowly – as precluding only the imposition of obligations on IAPs to engage in *indiscriminate* filtering of the electronic communications of *all* of its subscribers, *entirely* at their

[158] In relation to a technical obligations code, "subscriber appeal" means an appeal by a subscriber in relation to the proposed taking of a technical measure, or any other act or omission in relation to a technical obligation or a technical obligations code (section 124N CA).
[159] Section 124J(1)(b); section 124K(2)(a) and (10) CA.
[160] Section 124H(3) and (4) CA.
[161] See e.g. the remarks of the Joint Committee on Human Rights on the equivalent provisions of the Digital Economy Bill: "Legislative Scrutiny: Digital Economy Bill" (HL Paper 44; HC 327), 5 February 2010.

own expense and for an *unlimited* period of time – and so as having no particular implications for the DEA's technical obligations regime. Yet there remains a significant risk that, if it becomes operational, that regime – albeit targeted at subscribers presumed to be repeat infringers, and partly funded by right-holders – will fail to balance relevant Charter rights in the manner required by the CJEU, and for this and other reasons fall foul of EU law; and that it will be widely perceived by Internet users as compromising their rights in particular, while also failing to reduce online copyright infringement significantly.

First of all, if invoked, the section 124H power would enable new sanctions to be imposed on subscribers in a way that would clearly engage Articles 7, 8 and 11 of the Charter (dealing respectively with the right to respect for one's private life and communications, to the protection of one's personal data, and to freedom of expression). If imposed, such sanctions would not only affect unlawful (albeit private and/or communicative) activities, but would also inevitably affect lawful activities, and thereby interfere with the ability of the subscriber and members of his/her household sharing the service to engage in work, education and the use of e-government services. Further, the sanctions would be imposed by IAPs, at the behest of copyright owners, and could be imposed without the prior involvement of a court or administrative authority; and this in turn would raise questions about the compatibility of the technical obligations regime with the Framework Directive. The subscriber would be able to bring an appeal to the independent appeals body, and from there to the First-tier Tribunal, before imposition; but should s/he not appeal within the specified timeframe, his/her Internet service could conceivably be curtailed by the IAP on the basis of unchallenged evidence submitted to the IAP by a right-holder. It is difficult to see how such a process could be the 'prior fair and impartial procedure' required by Article 1.3(a) of the Framework Directive.

Second, given the ease with which a determined computer cracker can break into even encrypted networks, the prospect cannot be discounted that technical measures will be imposed on large numbers of subscribers who will not in fact have infringed copyright at all. At the same time, subscribers who do engage in large-scale infringement – the very subscribers the regime aims to control – are highly likely to find ways to avoid the reach of technical measures entirely.[162] In short, implementation of the technical obligations regime risks provoking widespread allegations of unfairness, bias and lack of accountability on the part of the regime's main agents: the Secretary of State, OFCOM, right-holders, and IAPs. Intense critical scrutiny of the regime's efficacy would inevitably ensue, and this in turn would raise questions about whether the DEA creates new 'externalities' of its own: negative social consequences of copyright enforcement measures that are not paid for either by copyright owners, or by infringers. The UK Government has not so far seen fit to monetise the cost of any of these possible costs of implementing the DEA.[163]

[162] A preliminary study of the impact of the French Création et Internet legislation has found that since its introduction, infringing activity has actually increased by 3% among French Internet users, who have reacted to the new regime by finding alternative gateways to unlawfully uploaded online content that are outside the scope of the legislation's provisions: Sylvain Dejean, Thierry Pénard and Raphaël Suire, "Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français" (M@rsouin, CREM et Université de Rennes 1 (March 2010) (available at: http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf).

[163] BIS/DCMS, *Digital Economy Act: Impact Assessments* pp. 54-85.

Nonetheless, as the next Part explains, its strategy for distributing the costs that it *has* measured is particularly revealing of the regulatory strategy embedded in the DEA

5 COSTS, AND COST-SHARING

The Labour Government's initial thinking had been that right-holders and IAPs should bear an equal share of the expenditure incurred by IAPs in complying with their new obligations,[164] an arrangement broadly acceptable to right-holders. However, by January 2010 – doubtless under pressure from the ISP industry, which has consistently maintained that right-holders should cover all of the IAPs' costs – the then Business Secretary Lord Mandelson was indicating that right-holders would bear the 'largest part'[165] of these costs. This shift in position was reflected in the Labour Government's consultation paper of March 2010 on the cost-sharing issue,[166] which proposed that the cost to IAPs of processing CIRs, maintaining CILs and issuing notifications to subscribers be split roughly in the ratio 75:25 between right-holders and IAPs. The coalition Government decided to take forward this proposal, and to split not only these 'notification fees', but also the 'qualifying costs' (i.e. the costs incurred by OFCOM) and the 'case fees' (the costs incurred by the appeals body in dealing with subscriber appeals), in the same way.[167] It eventually finalised a first draft cost-sharing Order in September 2010, which, as required by Article 8(1) of the Technical Standards Directive, was notified to the European Commission.

However, the Commission questioned whether the imposition of qualifying costs and case fees on ISPs was compatible with Article 12(1) of the Authorisation Directive (AD).[168] Shortly thereafter Parker J. handed down his decision in *British Telecom*. The one ground on which he found in favour of the claimants concerned the compatibility of the draft cost-sharing Order with Article 12 AD. He held that qualifying costs (though not notification fees or case fees) would constitute "administrative charges" imposed on undertakings providing a network or service under the general authorisation, and that since these did not relate to any of the matters specified in Article 12, they would be unlawful.[169] Subsequently, OFCOM was asked to advise on options for reducing the cost of the appeals process. In the

[164] Memorandum by DCMS/BIS, published as Appendix I to the Delegated Powers and Regulatory Reform Committee's Second Report of 2009–10, para 27.
[165] Letter to the Chair of the Joint Committee on Human Rights from the Rt Hon Lord Mandelson, Secretary of State for Business, Innovation and Skills, 14 January 2010, published in JCHR, 'Legislative Scrutiny: Digital Economy Bill' 32.
[166] BIS, "Online Infringement of Copyright (Initial Obligations) Cost-Sharing" (March 30, 2010), (available at: http://www.bis.gov.uk/assets/biscore/business-sectors/docs/10-915-consultation-online-infringement-of-copyright.pdf).
[167] BIS, "Online Infringement of Copyright (Initial Obligations) Cost-Sharing: Government Response" (14 September 2010).
[168] Under that Directive, national regulatory authorities may impose administrative charges (e.g. to underwrite the costs of their regulatory work) on undertakings providing electronic communications services or networks under the general authorisation scheme. However, Article 12 allows only "the administrative costs … incurred in the management, control and enforcement of the general authorisation scheme" to be imposed on providers by way of charges, and then only in an "objective, transparent and proportionate manner".
[169] Ibid paras. 192-200.

light of that advice,[170] the DCMS concluded in August 2011 that appellants should be required to pay a fee of £20 (refundable in the event of a successful appeal) in order to minimise the risk of the system being disrupted by "vexatious or non bona fide appeals."[171] A second draft of the Online Infringement of Copyright (Initial Obligations)(Sharing of Costs) Order, re-written to reflect these developments,[172] has been re-notified under the TSD and is now expected to be laid before Parliament early in 2012. In the event of technical measures being introduced, the costs associated with these will be the subject of a separate consultation and Order.

It is the cost-sharing arrangements that most clearly reveal the de-centred regulatory strategy that underlies the online copyright infringement provisions of the DEA. To a copyright lawyer, accustomed to seeing copyright as a regime of private law, these arrangements will seem highly unusual: effectively, IAPs – who are third parties to any legal dispute between copyright owners and their subscribers – will be required to contribute to the cost of enforcing the former's private rights. Right-holders have relied on a range of arguments in support of this apparent anomaly. They point to profits allegedly lost due to file-sharing, and to the heavy investments they are already making in detecting these. They also claim that IAPs have indirectly benefited from the infringement possibilities Internet access offers, because these have increased demand for their services and enabled higher charges to be levied on file-sharing customers on the basis that they consume more bandwidth than other users. In addition they argue that IAPs will now benefit from controlling file-sharing because high bandwidth consumption slows data traffic through IAPs' networks, thereby threatening the efficiency of these networks; and that if IAPs were reimbursed in full for their costs they would have no incentive to minimise these costs and could even seek to inflate them. IAPs, meanwhile, have insisted that the Internet and those who provide access to it cannot be held responsible for increased copyright infringement, and that the finger of blame should be pointed instead at P2P software developers and sites that actively promote copyright infringement through file-sharing. The new enforcement framework, they argue, will only benefit right-holders, and passing the immediate costs of operationalising it on to right-holders would ensure that both its costs and its benefits are more fully taken into account and that the most efficient arrangements emerge.[173] It has also been suggested that IAPs will simply pass on their costs in the form of higher broadband charges for their subscribers, which could further widen the digital divide if lower-income users discontinue broadband or elect not to subscribe.

The view taken by both the Labour and the coalition Governments has been that making IAPs bear some of the costs would not only incentivise them to comply

[170] OFCOM, "Digital Economy Act Online Copyright Infringement Appeals Process: Options for Reducing Costs" (3 August 2011).

[171] DCMS, "Next Steps for Implementation of the Digital Economy Act" p.6. Under section 124M(2)(c) CA, the Secretary of State has the power to specify in the cost-sharing Order the fees, if any, that are payable by subscribers in respect of subscriber appeals. The Government took the view that a no-fee regime might find itself the target of an orchestrated campaign by those opposed to the measures, and that a large volume of such 'protest' appeals could drive up the cost of the appeals process to the point where it became unworkable.

[172] Available at: http://www.culture.gov.uk/publications/8365.aspx.

[173] Mott McDonald Group, "P2P Report" (February 2010) pp.18-20, http://webarchive.nationalarchives.gov.uk/20100511084737/interactive.bis.gov.uk/digitalbritain.

efficiently with their notification and listing obligations, but also to act voluntarily to reduce online copyright infringement (thereby reducing the number of notifications they might have to process) and to enter into joint ventures with copyright owners to provide access to lawful content "under which a bilateral agreement could reduce the numbers of notifications they receive."[174] To this extent, the cost-sharing element of the new system is absolutely integral to what is arguably the overall goal of sections 3-16: to prompt (while not directly commanding) the emergence of new online business models for lawful content, and a degree of vertical integration between content providers and Internet access providers.

6 CONCLUSION

Although self-regulation and co-regulation (in the senses outlined in Part 2.1 above) were originally favoured by the UK Government as ways of managing the phenomenon of online copyright infringement, neither the initial obligations regime nor the technical obligations regime envisaged by sections 3-16 DEA could be described as either self- or co-regulatory: between them, the Secretary of State and OFCOM are to formulate every detail of each regime. Yet mechanisms of regulatory intervention are nonetheless bound to be highly fragmented in the practical operation of the DEA, with copyright owners, IAPs, and even subscribers themselves (along with ICT security firms purveying encryption, tracking and related products and services) all having some role to play. This fragmentation is inevitable given the grand ambition that appears to underlie this legislation: to trigger new patterns of interaction between content providers, IAPs and consumers that will ultimately restructure the market for digitised cultural content. However, there are evident difficulties associated with 'outsourcing' regulation in this manner, particularly where cyberspace is concerned. Not the least of these is ensuring that all the envisaged participants have read the script and can be counted on to play their assigned parts. There are clear signs that at least some of the large IAPs – whose informational resources, strategic position vis-à-vis end-users, organisational capacities and technical facilities would be crucial to the DEA's successful implementation – will strenuously resist being enrolled as the copyright industries' private police force. The main motivations prompting the two largest UK IAPs to seek judicial review of the DEA were that it would impose disproportionate costs on them – not only a share of its quantifiable operating costs, but other costs incurred through loss of custom and damage to goodwill. They anticipate these losses because many Internet users experience the Intenet not primarily as the locus of failure-prone information markets that deserve legal support on economic grounds, but as a site of cultural development and identity-formation in which the integrity of communication takes priority over the imperatives of commerce. These users will certainly resist any curtailment of freedoms that have not only become habitual, but are increasingly coming to be regarded as grounded in individual rights. Resistance could involve circumventing the measures applied by IAPs,[175] deluging IAPs with complaints, or migrating to other IAPs that are not obliged to apply the measures. And while such reactions are indeed likely to involve monetary losses for IAPs, their organisational cultures may in any

[174] BIS, "Online Infringement of Copyright (Initial Obligations) Cost-Sharing", p.15.
[175] The detection of IP addresses can be avoided by, for example, using proxy addresses and proxy servers, or by encrypting peer-to-peer transmissions.

case incline IAPs to sympathise with their subscribers' grievances – after all, TalkTalk's 'Don't Disconnect Us' campaign against the Digital Economy Bill was run entirely on the basis that it threatened Internet users' civil liberties.

End-users' values and reactions are not only likely to inform IAPs' approach to the new regime: the cultural industries cannot afford to ignore them either, and for at least two reasons. First, many Internet users are highly tech-savvy, and previous experience with DRM shows that there are few, if any, restrictions on Internet use that cannot sooner or later be broken through or routed around. Second, at the heart of the cultural industries' operations lies an ineradicable contradiction: their profitability depends on, even as it is undermined by, unrestricted access to and enjoyment of cultural commodities. On one hand, the value of a cultural commodity depends on the size of its audience, because the bigger the audience the greater the 'buzz' that in turn produces hits and stars. So it is that a senior executive of one of the 'big four' global music corporations can assert that "our vision is music availability everywhere, at any time and in any place."[176] On the other hand, audiences take shape in the exercise of freedoms to experience cultural commodities and communicate (through) them, freedoms that are impossible for the industries fully to manage or monetise but which only exist *as* freedoms in so far as they are not fully manageable or monetisable. Because of the nature of digital technology, every use and transmission of a cultural commodity online can involve taking and re-circulating intellectual property, and so eat directly into profits unless controlled and metered – hence the current concerns about mass online copyright infringement. Yet once the unfettered use and transmission of cultural commodities is seen for what it is – as an inevitable adjunct of cultural consumption in the digital networked environment – it becomes clear that the cultural industries eradicate it at their peril.

[176] Eric Daugan, Warner Music International (quoted in IFPI *Digital Music Report 2010*, p. 4, available at: http://www.ifpi.org/content/library/DMR2010.pdf).