

The Digital Economy Act 2010: Is the DEA DOA?

Michael Filby [\[1\]](#)

Cite as: Filby, M., 'The Digital Economy Act 2010: Is the DEA DOA?', European Journal of Law and Technology, Vol. 2, No.2, 2011

ABSTRACT

The *Digital Economy Act 2010* was hurried into existence in the dying days of the last Labour government, and contains powers designed to resist unauthorised file sharing that are due to be implemented by an Initial Obligations Code authored by Ofcom. Even before the Code has been published, there are several pre-existing key areas of the Act that contain significant evidential problems and potential incompatibilities with existing law. This paper critically reviews the legislation and identifies a number of significant flaws in consideration of its ongoing judicial review and the regulatory review by Ofcom. The status of the DEA in light of the recent decision in *MediaCAT v. Adams* is also discussed in the context of the threat it contains to the fundamental evidential foundation upon which the operation of the Act is based.

1. INTRODUCTION

The *Digital Economy Act 2010* (DEA) was rushed into the statute books shortly before the general election in May 2010, bringing with it a new regime designed to operate alongside the existing measures available in the *Copyright, Designs and Patents Act 1988* (CDPA) with the purpose of reducing unauthorised file sharing. The Act was initially due to be implemented by an Initial Obligations Code authored by Ofcom in late 2010, but has met with delay due to overwhelming academic and industry criticism that has culminated in a judicial review initiated by internet service providers (ISPs) TalkTalk and BT. This paper provides a critical review of the Act, and identifies flaws in the legislation regarding the proposed infringement notification procedure, its associated subscriber appeals process and compatibility with EU law. The impact of the recent case of *MediaCAT v. Adams* on the Act is considered in light of the serious evidential issues raised within it that potentially bear a direct and significant impact on the operation of the regime set up by the Act.[\[2\]](#) It is concluded that the DEA should not be implemented until it is subjected to considerable reform that will satisfactorily address the issues raised in *MediaCAT* and the ongoing judicial review.

2. THE DIGITAL ECONOMY ACT 2010

The DEA contains a number of sections that deal with matters such as changes to the role of Ofcom in overseeing media regulation [\[3\]](#), domain name registry regulation [\[4\]](#), and miscellaneous provisions relating to intellectual property including the granting of the right for libraries to lend e-books and audio

books [5]. In response to the Gowers Review of Intellectual Property [6], the Act also raises the maximum penalty for criminal infringement of copyright [7], but a controversial clause allowing orphan works to be used without being an infringement if the author cannot be traced that would also have addressed a recommendation of the Review [8] was removed. [9] The online infringement of copyright is dealt with in ss. 3-18 DEA 2010. Ss. 3-16 of the Act inserts ss.124A-N into the *Communications Act 2003*.

2.1. INFRINGEMENT NOTIFICATION PROCEDURE

S.3 of the Act provides an obligation to notify ISP subscribers of reported infringements. [10] If it 'appears' [11] to the copyright owner that a subscriber has infringed their copyright [12] or 'allowed another person to use the service' to infringe their copyright [13], then the owner can submit a copyright infringement report to the ISP once the obligation has been codified by Ofcom [14]. Within a month of receiving the report, the ISP must send a notification to the subscriber [15] containing the information included in the infringement report. The Act specifies that these notifications can be carried out via the postal address or e-mail address of the subscriber [16].

It is surprising that the Act permits notifications to be sent via e-mail, as this is a far less reliable means of communication than the traditional postal mail system. There is a risk that notifications sent by e-mail will not be seen by the intended recipient if they are, for example, inadvertently filtered out by anti-spam software or if the subscriber simply does not use the e-mail address provided by their ISP. If this should occur, the subscriber could lose the opportunity to appeal these notifications. It would consequently be more appropriate for notifications to be sent exclusively by registered postal mail. At the time of writing, the draft Code initially prepared by Ofcom does not recognise this problem as it specifies that the first and second copyright infringement notices may be sent by e-mail. Only the third notice must be sent by recorded postal mail, at which point the alleged infringer will be subject to sanction or having their details revealed to the copyright holder. [17]

The obligation on ISPs to provide infringement lists to copyright owners, as initially referenced in s.3(8) (a) DEA 2010, is expounded upon in s.4. [18] A copyright infringement list is defined as a list that identifies which subscribers have been subject to copyright infringement reports issued by the owner requesting the list [19] once the subscribers have been subject to the number of infringement notices stipulated as the threshold limit within the Code. [20] The list can be requested by copyright owners when the Initial Obligations Code granting this right is adopted. [21] At this stage, the identity of the specific subscribers must be kept anonymous. [22]

This section has been drafted in an attempt to maintain compatibility with Articles 12-14 of the *E-Commerce Directive* which provide explicit protection for ISPs in order to preserve their ability to maintain the proper functioning of and access to the internet. [23] This protection is maintained through offering an immunity from liability to ISPs which act as a mere conduit or internet intermediary and only cache or host information, provided they do not exercise any control over that information. [24] This protection is recognised by the Department for Business, Innovation and Skills (BIS, formerly BERR). [25] Article 15 prohibits Member States from imposing an obligation upon such ISPs to monitor the activities of their subscribers:

'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.' [26]

The Directive contains a caveat to this, in that Member States may establish obligations for:

'... information society service providers to promptly inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.' [27]

By utilising this caveat, the obligation to provide infringement lists to copyright owners essentially introduces ISP monitoring indirectly.

In the initial stages of the judicial review of the Act [28], it was submitted by the claimants that this falls under the definition of monitoring for the purposes of the Directive. [29] Further, even if this mechanism cannot be considered to fall within the technical definition of monitoring provided by the Directive, the necessary administration of the indirect monitoring process required by the Act still raises the question of whether the information involved can be deemed to be personal data in the context of the *Privacy in the Electronic Communications Sector Directive* (PEC Directive). [30] It is argued by the claimants that the contents of the copyright infringement reports and lists constitute personal data as they can identify the racial or ethnic origin, political opinions, religious or philosophical beliefs and health or sexual preferences of a subscriber. [31] If this is the case, then it is suggested by the claimants that the requirement for the ISPs to process this data falls foul of the privacy and proportionality requirements of the *PEC Directive* and the *Data Protection Directive*. [32] Although the defendants countered this argument with the contention that it was recognised in *Promusicae* [33] that the *PEC Directive* does not preclude Member States from laying down an obligation to disclose personal data in the context of civil proceedings, the claimants pointed out the process required by the DEA is not a civil proceeding in that no judicial oversight is involved, nor is the extent and ambit of the disclosure tailored to the individual circumstances of each case as a result of the exercise of regulatory judgment by an administrative authority [34]. It was also noted that European Data Protection Supervisor, Peter Hustinx, [35] submitted the opinion when considering the three strikes regimes under ACTA [36] that the monitoring of the behaviour and collection of IP addresses of internet users constitutes an interference in their right to a private life and correspondence, [37] and that IP addresses should be considered to be personal data. [38]

2.2. INITIAL OBLIGATIONS CODE

Ss.5-7 of the Act [39] pave the way for the drafting and adoption of the Initial Obligations Code through which Ofcom will oversee the operation of the *Digital Economy Act*. In addition to stipulating the conditions for approval of a Code about the initial obligations [40] and establishing of the Code itself along with provisions relating to the jurisdiction and function of Ofcom to adapt to this [41], the contents of the Initial Obligations Code are specified. [42] The costs of the administration and enforcement carried out by Ofcom must be met by both the copyright owners and, unusually, the ISPs. [43] There is further provision for fines to be levied in the event of non-compliance with the Code. The decision to apportion responsibility for a share of the costs to the ISPs was proposed by Baroness Howe of Idlicote, who described the copyright holders as victims not taken seriously by the ISPs in their plight. [44] Lord Young of Norwood Green shone a different light upon the clause in pointing out that

'... we feel that ISPs should share some of the burden to ensure that they carry out their obligations in an efficient and economic manner and have an incentive both to reduce infringement and to participate in business models.' [45]

This latter argument was supported in the Cost Sharing portion of the Government Response. [46] It stated that 'sharing appeal costs between ISPs and copyright owners provides a further incentive to

ensure the processes are as robust as possible.' [47] Submissions by the ISPs to the same consultation pointed out that they would not require any additional incentive to keep their operating costs to an absolute minimum, as operating with maximum profitability is their sole purpose of being. [48]

The major ISPs and several consumer groups raised several objections in their respective responses to the initial consultation, arguing that, unlike the copyright owners, ISPs have no direct control over the carrying out of the operation of the Act nor do they enjoy any benefit from it. [49] They also pointed out that any costs statutorily assigned to the ISPs would be inevitably passed along to their customers. Despite these concerns, BIS announced in the Government Response that their intention is to split the costs so that rights holders will pay just 75% of the costs, whereas ISPs (and thus subscribers) will pay 25%. [50] Further, Ofcom announced that the Code will only initially apply to ISPs with more than 400,000 subscribers as this will cover 96.5% of the residential and small to medium sized business broadband market. [51] Ofcom argues that this will therefore cover the largest proportion of unauthorised file sharers. [52] This could encourage those wishing to avoid the gaze of the Code to simply migrate to a smaller ISP.

The Code must be kept under review, according to s.8 *DEA 2010*, via interim reports prepared every 3 months [53] and full reports prepared every 12 months [54] by Ofcom. Although both the full reports and interim reports must contain an assessment of the level of infringement being carried out by subscribers, it is not specified how such assessments are to take place. [55] There is also no guidance in the Act pointing out how to define what constitutes a 'substantial' level of infringement. It is particularly important that this is defined as it is presently uncertain if the unauthorised downloading of, for example, a music album would be construed as a single infringement or a multiple infringement of ten or more single music tracks.

2.3. TECHNICAL MEASURES

The Act provides that assessment and preparation must be carried out before what the Act terms as technical obligations and technical measures can be imposed. These technical measures, particularly the prevention of the subscriber from accessing particular material and disconnection from the internet, have been the greatest cause of contention among critics of the Act for a number of reasons. For instance, there is no existing method to block particular areas of the internet or specific material in a way that cannot be easily bypassed by those with sufficient technical knowledge. There is also a growing feeling amongst an increasing number of international bodies that access to the internet and its accompanying services is to be considered a fundamental or human right. Although the European Union has yet to adopt a unified stance on this point, this notion has already been accepted by European states such as France (according to the Constitutional Council citing the *French Declaration of 1789*) [56], Greece (which added the right to participate in the information society in the 2001 revision of the Constitution of Greece) [57], and Finland (where the Finnish Ministry of Transport and Communications announced in 2009 that from July 2010, every citizen will have the right to access a 1Mb broadband connection). [58] Arguments have also been put to the United Nations, at the World Summit on the Information Society, that this should be adopted as a general principle. [59] The UN Special Rapporteur has recently issued a report considering the right to freedom of opinion and expression, which concludes that disconnection on the grounds of violating intellectual property rights law is a violation of Article 19(3) of the *International Covenant on Civil and Political Rights*. [60]

It has been argued by the claimants in the judicial review of the DEA that these technical obligations, along with several other requirements of the Act, are contrary to the *Technical Standards Directive* [61] in that the European Commission was not notified of the technical regulations imposed

upon ISPs by the DEA prior to its passing. [62] This was initially countered by the defendants with the contention that the Act is merely an enabling provision on account of the fact that an Initial Obligations Code is required to bring the full powers of the Act into force. However, the claimants pointed out that the authority relied upon for this line of argument, the case of *CIA Security International*, [63] was pursuant to the predecessor Directive to the *E-Commerce Directive* [64] and thus the definition provided there is no longer applicable, as affirmed in *Liga Portuguesa de Futebol Profissional*. [65] The claimants also argued that the technical obligations and other measures to be set out in the Initial Obligations Code have been largely prescribed to the extent that they are not subject to further substantial amendments:

'The Act has set down the form which technical measures, if introduced, will take. There is now no possibility of suggesting that alternative, less restrictive technical measures should be introduced instead. Nor can the Commission or other Member States have any input into what the substantive nature of the technical measures should consist in, or whether non-technical measures such as education campaigns, improvement of civil procedures and so on might be considered instead. In addition, the appeal mechanism for subscribers has been set. There is already an in-built presumption that a subscriber is responsible for traffic over his or her internet connection and a duty exists to take reasonable care to protect it. The presumption has also been fixed that the subscriber committed any established copyright infringement, unless he or she proves the contrary.' [66]

If it is found that these sections of the DEA do indeed fall within the definition provided by the Directive, they could potentially be rendered unenforceable.

2.4. SUBSCRIBER APPEALS PROCESS

Concerns were frequently raised during the pre-Act consultation period regarding the evidential standard to be imposed and the inherent danger of the infringement detection methods used by the copyright owners being inaccurate. The Act attempts to address these concerns with the establishment of a subscriber appeals process to be provided for in the Code. [67] Although the onus is on the copyright owner to establish that there was an infringement of copyright and that the infringement took place via an IP address belonging to the subscriber at the time of the infringement, [68] to counter the contention of the copyright owner the Act requires the subscriber to show not only that they did not commit the alleged infringement, but also that they took 'reasonable steps' to prevent other persons from infringing copyright using their account. [69]

The BIS has indicated that access to the appeals process will potentially be free of charge to the subscriber in the first instance, but this is accompanied by the caveat that the power to introduce a fee will be retained if there is a 'significant number of vexatious appeals' or when technical measures are introduced. [70] Any future requirement for the subscriber to pay to access the appeals process should ideally be avoided, as this could dissuade those innocently accused of infringement from appealing for fear of losing the required fee. A fairer system would see free access to the appeals process alongside a power granted to the overseer of the appeal to levy a fine upon rights holders who make false claims, similar in nature to that suggested by the Open Rights Group [71].

There is also still a great deal of uncertainty with regard to the evidential standard required to trigger a copyright infringement report. Although the Act specifies that the burden of proof during the appeals process is on the copyright owner, the subscriber may not be successful in an appeal by merely showing that the infringement was not committed by them, but must further show that they have taken 'reasonable steps' to prevent other persons from infringing copyright through the use of their account.

Although it is not specified what these reasonable steps should entail, provisions such as s.3(6)(h) DEA 2010 (which requires that infringement notifications sent to subscribers should include information on 'steps that a subscriber can take to protect an internet access service from unauthorised use') indicate that the subscriber must show that they have secured their wireless connection. If this interpretation is correct, then liability is created for the ISP account holder for anybody who has used their account with or without their permission.

This lies in contrast with the existing duties under the CDPA that have recently been considered in *MediaCAT v. Adams*. [72] This case involved the harvesting of IP addresses from trackers purportedly linked with torrent swarms of infringing content. After obtaining the IP addresses, *Norwich Pharmacal* [73] orders were applied for by, and granted to, the plaintiffs through the High Court requiring several ISPs to reveal the details of the subscribers recorded as being associated with those IP addresses at the time of the alleged infringements. ACS:Law then sent letters en masse to the subscribers demanding various amounts, usually in the region of £495, accompanied by the threat of litigation in the event of non-payment. [74] This particular case was one of the first and only attempts made by ACS:Law and its partner firm MediaCAT to carry out their threat of litigation for copyright infringement, and was carried out against 26 of these alleged infringers who refused to pay. Several arguments were put forward by the claimants suggesting that the liability of subscribers for infringements that have allegedly taken place utilising their connections established in the DEA already existed under the CDPA, but this view was rejected by HH Judge Birss:

'It is not at all clear to me that the person identified must be infringing one way or another. The fact that someone may have infringed does not mean the particular named defendant has done so.' [75]

This is consistent with the claim made by BERR in its pre-consultation document for a digital rights agency that 'the fact that a particular internet address has been used will probably not be enough to [identify the defendant] given the possibility of wireless connections to that address.' [76] However, it should be remembered that this ruling relates to the procedure that has been interpreted from the framework of the CDPA. In contrast, the DEA sidesteps this problem by apparently creating a new duty for the account holder that will hold them accountable for the activities of any other person using the connection. This carries with it the unfortunate side effect of effectively outlawing the open WiFi initiatives that are frequently offered by educational establishments such as universities and libraries, and businesses such as pubs, cafes and restaurants, and could easily be accompanied by a curtailing of the speed at which blanket coverage of wireless internet access is offered across the country. [77]

Less easily avoided is the question also raised in *MediaCAT v. Adams* that asks whether the IP address obtained by the rights holder does in itself 'establish that any infringement of copyright has taken place by anyone related to that IP address at all.' [78] The defendants identified several frailties associated with the current means of obtaining IP addresses from BitTorrent trackers, namely that trackers are not assiduous in keeping their lists up to date, that IP addresses get reallocated, and that a particular IP address may be obtainable from a tracker even if the person using it had stopped a download immediately after starting it (whereby such a small amount of information would have been downloaded as to be legally irrelevant). [79] Although these points were not explicitly ruled upon in this instance due to their technical nature, it was recognised that it has never been established whether this approach to identifying IP addresses does in fact reveal that copyright infringement has actually taken place.

In terms of establishing a standard of proof for rights holders under the auspices of the DEA in contrast to the CDPA, it must be established in the former merely that it 'appears' that an infringement has taken place. The rationale for this choice was explained by Lord Whitty as making an accusation of infringement 'less harsh', 'more neutral' and 'less threatening'. [80] However, it is difficult to ignore the

possibility that this nebulous standard seemingly recognises that the key step in a procedure that will lead to the identity of a possibly innocent subscriber being revealed to rights holders is based upon an evidentially weak system of monitoring. Should the arguments against the veracity of IP addresses obtained by monitors be accepted in a future hearing, the task of the copyright owner in establishing that an infringement took place via an IP address belonging to the subscriber at the time of the infringement could become unworkably difficult. [81] Further rulings on the efficacy of current monitoring techniques in linking an IP address to an infringement will thus prove crucial to the operation of the DEA.

2.5. WEB BLOCKING

Following ancillary provisions regarding the enforcement of the obligations the Act exerts upon ISPs with the threat of a fine of up to £250,000 for non-compliance, [82] formalisation of the requirement for costs to be shared by copyright owners, ISPs and subscribers, [83] and various minor interpretative clarifications, [84] comes the suggested power to make provisions about injunctions preventing access to locations on the internet. [85] This section provides that a court may grant an injunction which requires ISPs to block access to an area of the internet if the court is satisfied that the location 'has been, is being or is likely to be used for or in connection with an activity that infringes copyright'. [86] This provision to block sites is worded widely. The somewhat oblique requirement that a site can be blocked if it is 'likely' to be associated with an activity connected with infringing copyright, along with the lack of a definition as to what may constitute 'substantial infringement', would have left a great many websites susceptible to being subject to a blocking injunction. For example, Wikileaks, YouTube and the Google search engine all fall within this definition of a site eligible to be blocked, as do facilities offering new digital business models such as online locker services. [87]

However, the entire power to grant site blocking injunctions was stymied by the last minute requirement for consultation and parliamentary scrutiny to be held prior to s.17 DEA 2010 coming to force. [88] This requirement was added after the Bill left the House of Lords as a concession to critics of the section who felt that such a significant power should not have been included in an Act that was not subject to the level of parliamentary scrutiny usually afforded due to the wash-up process. This was followed up by a review of the feasibility of such powers by Ofcom, requested by Culture Secretary Jeremy Hunt. [89] It accurately concluded that site blocking would not be effective due to the ease at which it can be bypassed. [90] As a result it has been announced that these potentially damaging provisions of the DEA will not be implemented, [91] although the pre-existing s.97A CDPA 1988 still offers a route to site blocking via the courts. [92]

3. CONCLUSION

As a piece of legislation designed to implement the recommendations of the Gowers Review of Intellectual Property, [93] the legislature has taken a one-sided view. Several recommendations relating to the enforcement of certain powers desired and lobbied for by rights holders have been implemented in the Act, including increasing the awareness of what is described as 'IP crime', [94] the matching of penalties for online infringement with physical infringement, [95] and the removal and disbaring of internet users 'engaged in piracy'. [96] However, the legislature has declined to implement any of the recommendations designed to bring copyright law into line with the realities of the digital economy, such as introducing a limited private copying exception to allow format shifting [97] or paving the way for a system of labelling products with DRM attached to them so that consumers can identify when digital

intellectual property they are purchasing is incompatible with certain devices or requires an open internet connection to which they may not have access. [98] Indeed, the closest the legislature came to recognising the true nature of the digital economy was with the introduction of the clause making provision for the use of orphan works. [99] However, the poor drafting of the legislation and the brief amount of time available to discuss and amend the Act, as well as the fact that no preparatory steps had been taken (such as the establishing of 'reasonable search' parameters [100] and a voluntary copyright register, [101] as recommended in the Gowers Review), led to the clause being withdrawn before the Act was passed.

The most vocal bodies that have expressed support for the new legislation are the rights holders and their lobbyists. [102] Those that are in opposition to the Act include ISP subscribers [103] and their representative consumer groups [104], the ISPs that are concerned with the costs that they will incur for regulations that will alienate their own customer base, [105] and the police and security service who have both expressed concern that the effect the Act will have in persuading internet users to routinely encrypt their internet use will make monitoring communications in their criminal law enforcement roles more difficult. [106]

There is nothing in this section of the *Digital Economy Act* that recognises or supports new digital business models. There is, however, an abundance of provisions that preserve outmoded analogue business models that will, in their current form, impede key areas of technological evolution such as the increasing reach of open WiFi. Yet the lack of attention the Act received prior to its passing is now being made up for in post-legislative scrutiny that could effectively paralyse its new regimes. For example, the ongoing judicial review of the DEA has already served to delay the implementation of the finalised Initial Obligations Code. If the monitoring obligations, technical measures and handling of data required by the Act are eventually found not to be compatible with the corresponding European legal framework, or if the measures are found to be disproportionate or contrary to human rights protections, key sections of the Act could be rendered unenforceable.

What is certain is that conclusions will not be reached quickly, and the continuing judicial review process will at the very least delay implementation further. There also remains the separate threat to the evidential basis of the infringement notification procedure. Although the crucial exploration that was taking place in *MediaCAT v. Adams* stalled due to the collapse of plaintiff firms MediaCAT and ACS:Law, any future challenge could see this crucial element of the new regime fatally undermined. If it cannot be legally assumed (as it cannot be technically) that scraping IP addresses from BitTorrent trackers proves that infringing activity has taken place from the account of an associated subscriber, the sole basis of the three strikes scheme laid out so haphazardly in the Act will be disabled, effectively crippling the so-called graduated response process itself. Even if the DEA manages to dodge the bullet of legal paralysis, it is unlikely to have any meaningful effect on piracy due to its failure to acknowledge that the majority of file sharers can utilise technical knowledge to avoid its reach with great ease. [107] Whether the Act is defeated technically or legally, it is doubtful that it will ever come to be applied in its current form with any consequential degree of efficacy.

[1] Michael Filby LLB, LLM, MPhil is a former lecturer in law and legal researcher with the University of Hertfordshire.

[2] *MediaCAT v. Adams* [2011] EWPC 006 .

- [3] DEA 2010 ss.1-2.
- [4] DEA 2010 ss.19-21.
- [5] DEA 2010 s.43.
- [6] A Gowers, Gowers Review of Intellectual Property (The Stationery Office, London 2006), Recommendation 36.
- [7] DEA 2010 s.42.
- [8] Ibid Recommendation 13.
- [9] Committee of the Whole House HC (7 April 2010)<http://www.publications.parliament.uk/pa/cm200910/cmbills/089/amend/pbc0890704m.1319-1325.html> accessed October 2011.
- [10] Inserting Communications Act 2003 s.124A.
- [11] DEA 2010 s.3(1).
- [12] DEA 2010 s.3(1)(a).
- [13] DEA 2010 s.3(1)(b).
- [14] DEA 2010 s.3(1)(2).
- [15] DEA 2010 s.3(5).
- [16] DEA 2010 s.3(9).
- [17] Ofcom, 'Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code' (Ofcom 2010)<http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf> accessed October 2011, ss.5.5, 5.6 & 5.8 at pp.50-51.
- [18] Inserting Communications Act 2003 s.124B.
- [19] DEA 2010 s.4(2)(a).
- [20] DEA 2010 s.4(3).
- [21] DEA 2010 s.4(1)(b).
- [22] DEA 2010 s.4(2)(b).
- [23] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ [2000] L No. 178, 17.7.2000, as enacted by The Electronic Commerce (EC Directive) Regulations 2002, S.I. 2002/2013.
- [24] Defined in similar terms to the safe harbours outlined in the US Digital Millennium Copyright Act 1998 s.512.
- [25] BIS, Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing (The Stationery Office, London 2008) 17-18, paras.3.32-3.35.
- [26] E-Commerce Directive art 15(1).
- [27] E-Commerce Directive Art.15(2).

- [28] R (on the application of British Telecommunications and TalkTalk Telecom) v. Secretary of State for Business, Innovation and Skills [2011] (Unreported).
- [29] 'The Queen on the application of (1) British Telecommunications Plc (2) TalkTalk Telecom Group Plc and The Secretary of State for Business, Innovation and Skills: Statement of Facts and Grounds' (TalkTalk 2011) <http://www.talktalkblog.co.uk/2010/07/08/judicial-review-of-the-digital-economy-act/> accessed October 2011, Paras.120-154.
- [30] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ [2002] L No. 201.
- [31] 'The Queen on the application of (1) British Telecommunications Plc (2) TalkTalk Telecom Group Plc and The Secretary of State for Business, Innovation and Skills: Statement of Facts and Grounds' (TalkTalk 2011) <http://www.talktalkblog.co.uk/2010/07/08/judicial-review-of-the-digital-economy-act/> accessed October 2011, Para.166.
- [32] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ [1995] L No. 281, 23.11.1995,
- [33] Case C-275/06 Productores de Música España (Promusicae) [2008] ECR I-271, ECJ.
- [34] 'The Queen on the application of (1) British Telecommunications Plc (2) TalkTalk Telecom Group Plc and The Secretary of State for Business, Innovation and Skills: Statement of Facts and Grounds' (TalkTalk 2011) <http://www.talktalkblog.co.uk/2010/07/08/judicial-review-of-the-digital-economy-act/> accessed October 2011, Para.173.
- [35] Ibid FN 34 para.177.
- [36] Anti-Counterfeiting Trade Agreement.
- [37] Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), (2010/C 147/01), Para.24.
- [38] Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), (2010/C 147/01 para.25.
- [39] Inserting Communications Act 2003 ss.124C-E.
- [40] DEA 2010 s.5.
- [41] DEA 2010 s.6.
- [42] DEA 2010 s.7.
- [43] DEA 2010 s.7(8).
- [44] Hansard HL vol 717 col 1494 (3 March 2010), <http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100303-0008.htm> accessed October 2011.
- [45] Hansard HL vol 717 col 1496 (3 March 2010), <http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100303-0008.htm> accessed October 2011.

[46] BIS, 'Online Infringement of Copyright (Initial Obligations) Cost Sharing: HM Government Response September 2010' (Department for Business, Innovation and Skills 2010) <http://www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response> accessed October 2011.

[47] Ibid 3.

[48] Ibid 5.

[49] Ibid pp.5-6.

[50] BIS, 'Online Infringement of Copyright (Initial Obligations) Cost Sharing: HM Government Response September 2010' (Department for Business, Innovation and Skills 2010) <http://www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response> accessed October 2011.

[51] Ofcom, 'Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code' (Ofcom 2010) <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf> accessed October 2011, para.1.6, p.2 & paras.3.14-3.15, pp.12-13.

[52] Ofcom, 'Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code' (Ofcom 2010) <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf> accessed October 2011, para.1.6, p.2 & paras.3.14-3.15, pp.12-13 para.3.15, p.12.

[53] DEA 2010 s.8(3).

[54] DEA 2010 s.8(2).

[55] DEA 2010 s.8(5).

[56] See C Bremner, 'Top French Court Rips Heart out of Sarkozy Internet Law' (The Times 2009) http://technology.timesonline.co.uk/tol/news/tech_and_web/article6478542.ece accessed October 2011; & I Sparks, 'Internet Access is a Fundamental Human Right, Rules French Court' (The Daily Mail 2010) <http://www.dailymail.co.uk/news/worldnews/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html> accessed October 2011.

[57] Art.5A;

see <http://web.archive.org/web/20030427062355/http://www.vouli.gr/politeuma/syntagmaDetails.asp?Arthroid=6> accessed October 2011.

[58] See YLE, '1Mb Broadband Access Becomes Legal Right' (Finnish Broadcasting Company 2009) http://www.yle.fi/uutiset/news/2009/10/1mb_broadband_access_becomes_legal_right_1080940.html accessed October 2011.

[59] ML Best, 'Can the Internet be a Human Right?' (2000) Human Rights & Human Welfare 276.

[60] F La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (United Nations General Assembly 2011) http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf accessed October 2011.

[61] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ [1998] L No 204, 21.7.98, as amended by Directive 98/48/EC of the European Parliament and of the Council of

20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ [1998] L No 217, 5.8.98.

[62] 'The Queen on the application of (1) British Telecommunications Plc (2) TalkTalk Telecom Group Plc and The Secretary of State for Business, Innovation and Skills: Statement of Facts and Grounds' (TalkTalk 2011) www.talktalkblog.co.uk/2010/07/08/judicial-review-of-the-digital-economy-act/ accessed October 2011, Paras.51-119.

[63] CIA Security International [1996] ECR I-2201, ECJ.

[64] Directive 83/189/EEC of 28 March 1983 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ [1983] L No 109, 26.4.1983.

[65] Liga Portuguesa de Futebol Profissional v. Departamento de Jogos [2009] ECR I-0000, [2010] 1 CMLR 1.

[66] 'The Queen on the application of (1) British Telecommunications Plc (2) TalkTalk Telecom Group Plc and The Secretary of State for Business, Innovation and Skills: Statement of Facts and Grounds' (TalkTalk 2011) <http://www.talktalkblog.co.uk/2010/07/08/judicial-review-of-the-digital-economy-act/> accessed October 2011, Para.96.

[67] DEA 2010 s.13 (inserting Communications Act 2003 s.124J).

[68] DEA 2010 s.13(5).

[69] DEA 2010 s.13(6).

[70] BIS, 'Online Infringement of Copyright (Initial Obligations) Cost Sharing: HM Government Response September 2010' (Department for Business, Innovation and Skills 2010) accessed October 2011, 3.

[71] BERR, Government Response: Consultation on legislative options to address illicit Peer-to-Peer (P2P) file-sharing (The Stationery Office, London 2008), 4.

[72] MediaCAT v. Adams [2011] EWPC 006.

[73] Norwich Pharmacal Co. v Commissioners of Customs & Excise [1974] AC 133.

[74] For more on speculative invoicing in general, see A Murray, 'Volume Litigation: More Harmful than Helpful?' (SCL 2010) <http://www.scl.org/site.aspx?i=ed14683> accessed October 2011.

[75] MediaCAT v. Adams [2011] EWPC 006 para.91(ii).

[76] IPO, Copyright in a digital world: What role for a Digital Rights Agency? (The Stationery Office, London 2009), 21.

[77] B Farrand, 'The Digital Economy Act 2010 - a cause for celebration, or a cause for concern?' (2010) 32(10) European Intellectual Property Review 536, 539.

[78] MediaCAT v. Adams, para.91(i).

[79] MediaCAT v. Adams, para.7.

[80] Hansard HL vol 717 col 1287 (1 March 2010), see <http://services.parliament.uk/hansard/Lords/bydate/20100301/mainchamberdebates/part010.html> accessed October 2011.

[81] DEA 2010 s.13(5).

[82] DEA 2010 s.14(2).

[83] DEA 2010 s.15.

[84] DEA 2010 s.16.

[85] DEA 2010 s.17.

[86] DEA 2010 ss.17(1)-(2).

[87] R Fry, 'Forget the teenagers, we're all infringers now' (2010) 196 Copyright World 34.

[88] DEA 2010 s.18.

[89] Ofcom, 'Site Blocking' to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (Ofcom 2011) http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking_report_with_redactions_vs2.pdf accessed October 2011.

[90] Many of the simple and widely known ways to bypass site blocking were illustrated in the aforementioned Ofcom report, available without redactions at Ofcom, 'Site Blocking' to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (Ofcom 2011) <http://www.scribd.com/doc/61521898/Ofcom-Site-Blocking-Report-With-Redactions-Removed> accessed October 2011.

[91] BIS, 'Sweeping intellectual property reforms to boost growth and add billions to the economy' (Central Office of Information 2011) accessed October 2011.

[92] 20th Century Fox v. British Telecommunications [2011] EWHC 1981 (Ch).

[93] A Gowers, Gowers Review of Intellectual Property (The Stationery Office, London 2006).

[94] Gowers Review of Intellectual Property Recommendation 35.

[95] Gowers Review of Intellectual Property Recommendation 36.

[96] Gowers Review of Intellectual Property Recommendation 39.

[97] Gowers Review of Intellectual Property Recommendation 8.

[98] Gowers Review of Intellectual Property Recommendations 15-16.

[99] Gowers Review of Intellectual Property Recommendation 13.

[100] Gowers Review of Intellectual Property Recommendation 14a.

[101] Gowers Review of Intellectual Property Recommendation 14b.

[102] A Liversage, 'BPI Heralds Landmark Digital Economy Act, 8 April 2010' (British Phonographic Industry 2010) <http://www.bpi.co.uk/press-area/news-amp3b-press-release/article/bpi-heralds-landmark-digital-economy-act.aspx> accessed October 2011.

[103] More than 20,000 internet users e-mailed their representative members of parliament to express their opposition to the Bill before the final vote; see Tom Watson, who stated 'the 20,000 people who have taken the time to e-mail their MPs about the Bill in the past seven days are extremely upset that the Bill will not receive the scrutiny that it deserves and requires', at Hansard HC vol 793 col 837 (6 April 2010), <http://www.publications.parliament.uk/pa/cm200910/cmhansrd/cm100406/debtext/100406-0007.htm> accessed October 2011.

[104] The costs sharing element of the obligations code consultation included 11 ISPs, four consumer groups, two law societies, three individuals and a research organisation united in opposition of the Act against 16 rights holders; see BIS, 'Online Infringement of Copyright (Initial Obligations) Cost Sharing:HM Government Response September 2010' (Department for Business, Innovation and Skills 2010) <http://www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response> accessed October 2011.

[105] The internet commentator Stephen Fry on behalf of ISP TalkTalk stated, 'I'm no defender of systematic deliberate criminal downloading, but in my estimation the government's proposed Copyright Protection Law is ill-conceived, constitutionally outrageous, morally unfair and epically foolish. This is not the way to protect and strengthen the creative music, film and TV industries - it is a way further to alienate and antagonise the very people on whom those industries depend. Large scale criminal P2P downloaders will certainly be smart enough to avoid attention while the innocent or small-time (most of whom are good customers) will be penalised without recourse to the due process of the law'; at S Marinker, 'Digital Economy Bill Cannot Protect Copyright' (TalkTalk 2010) http://pressoffice.talktalk.co.uk/news/item/digital_economy_bill_cannot_protect_copyright/?phpMyAdmin=0f0a850a9f027986a254b43352595a5e accessed October 2011.

[106] P Foster, 'MI5 Comes Out Against Cutting Off Internet Pirates' (The Times 2009)<http://www.timesonline.co.uk/tol/news/uk/crime/article6885923.ece> accessed October 2011.

[107] For example, by employing the use of a virtual private network (VPN) that is hosted extra-jurisdictionally, or by utilising DHT which bypasses the use of BitTorrent trackers; see G Pratt, E Beazley and R Smith, 'All washed up: unauthorised file sharing and the UK Digital Economy Act 2010' (2010) Intellectual Property Magazine (June) 49; and Ofcom, 'Site Blocking' to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (Ofcom 2011)<http://www.scribd.com/doc/61521898/Ofcom-Site-Blocking-Report-With-Redactions-Removed> accessed October 2011.

BIBLIOGRAPHY

UK LEGISLATION

Communications Act 2003

Copyright, Designs and Patents Act 1988

Digital Economy Act 2010

EUROPEAN & INTERNATIONAL LEGISLATION

Constitution of Greece (2001

Revision);<http://web.archive.org/web/20030427062355/http://www.vouli.gr/politeuma/syntagmaDetails.asp?Arthroid=6> accessed April 2011

Directive 83/189/EEC of 28 March 1983 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ [1983] L No 109, 26.4.1983

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ [1995] L No. 281, 23.11.1995

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ [2000] L No. 178, 17.7.2000, as enacted by The Electronic Commerce (EC Directive) Regulations 2002, S.I. 2002/2013

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ [2002] L No. 201

Digital Millennium Copyright Act 1998 Pub. L. No. 105-304, 112 Stat. 2860 (US)

CASES

20th Century Fox v. British Telecommunications [2011] EWHC 1981 (Ch)

Case C-275/06 Productores de Música España (Promusicae) [2008] ECR I-271, ECJ

CIA Security International [1996] ECR I-2201, ECJ

Liga Portuguesa de Futebol Profissional v. Departamento de Jogos [2009] ECR I-0000, [2010] 1 CMLR 1

MediaCAT v. Adams [2011] EWPC 006

Norwich Pharmacal Co. v Commissioners of Customs & Excise [1974] AC 133

R (on the application of British Telecommunications and TalkTalk Telecom) v. Secretary of State for Business, Innovation and Skills [2011] (Unreported)

SECONDARY SOURCES

BERR, Government Response: Consultation on legislative options to address illicit Peer-to-Peer (P2P) file-sharing (The Stationery Office, London 2008)

ML Best, 'Can the Internet be a Human Right?' (2000) Human Rights & Human Welfare 276

BIS, Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing (The Stationery Office, London 2008)

BIS, 'Online Infringement of Copyright (Initial Obligations) Cost Sharing: HM Government Response September 2010' (Department for Business, Innovation and Skills 2010) <http://www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response> accessed April 2011

BIS, 'Sweeping intellectual property reforms to boost growth and add billions to the economy' (Central Office of Information 2011) <http://nds.coi.gov.uk/content/detail.aspx?NewsAreaId=2&ReleaseId=420683&SubjectId=16&AdvancedSearch=true> accessed October 2011

C Bremner, 'Top French Court Rips Heart out of Sarkozy Internet Law' (The Times 2009) http://technology.timesonline.co.uk/tol/news/tech_and_web/article6478542.ece accessed April 2011

Committee of the Whole House HC (7 April

2010)<http://www.publications.parliament.uk/pa/cm200910/cmbills/089/amend/psc0890704m.1319-1325.html> accessed April 2011

B Farrand, 'The Digital Economy Act 2010 - a cause for celebration, or a cause for concern?' (2010) 32(10) European Intellectual Property Review 536

P Foster, 'MI5 Comes Out Against Cutting Off Internet Pirates' (The Times 2009)<http://www.timesonline.co.uk/tol/news/uk/crime/article6885923.ece> accessed April 2011

R Fry, 'Forget the teenagers, we're all infringers now' (2010) 196 Copyright World 34

A Gowers, Gowers Review of Intellectual Property (The Stationery Office, London 2006)

Hansard HL vol 717 col 1287 (1 March 2010), see<http://services.parliament.uk/hansard/Lords/bydate/20100301/mainchamberdebates/part010.html> accessed April 2011

Hansard HL vol 717 col 1494 (3 March 2010), <http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100303-0008.htm> accessed April 2011

Hansard HL vol 717 col 1496 (3 March 2010), <http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100303-0008.htm> accessed April 2011

Hansard HL vol 718 col 481 (15 March 2010), see <http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100315-0006.htm> accessed April 2011

Hansard HC vol 793 col 837 (6 April 2010),<http://www.publications.parliament.uk/pa/cm200910/cmhansrd/cm100406/debtext/100406-0007.htm> accessed April 2011

HL, 'Digital Economy Bill' (House of Lords 2009) <http://www.publications.parliament.uk/pa/ld200910/ldbills/001/10001.13-19.html> accessed April 2011

F La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (United Nations General Assembly 2011) http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf accessed October 2011

A Liversage, 'BPI Heralds Landmark Digital Economy Act, 8 April 2010' (British Phonographic Industry 2010)<http://www.bpi.co.uk/press-area/news-amp3b-press-release/article/bpi-heralds-landmark-digital-economy-act.aspx> accessed April 2011

S Marinker, 'Digital Economy Bill Cannot Protect Copyright' (TalkTalk 2010)http://pressoffice.talktalk.co.uk/news/item/digital_economy_bill_cannot_protect_copyright/?phpMyAdmin=0f0a850a9f027986a254b43352595a5e accessed April 2011

A Murray, 'Volume Litigation: More Harmful than Helpful?' (SCL 2010) <http://www.scl.org/site.aspx?i=ed14683> accessed April 2011

Ofcom, 'Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code' (Ofcom 2010) <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf> accessed April 2011

Ofcom, 'Site Blocking' to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (Ofcom 2011) http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-report_with_redactions_vs2.pdf accessed October 2011

Ofcom, 'Site Blocking' to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (Ofcom 2011) <http://www.scribd.com/doc/61521898/Ofcom-Site-Blocking-Report-With-Redactions-Removed> accessed October 2011

Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), (2010/C 147/01)

G Pratt, E Beazley and R Smith, 'All washed up: unauthorised file sharing and the UK Digital Economy Act 2010' (2010) Intellectual Property Magazine (June) 49

I Sparks, 'Internet Access is a Fundamental Human Right, Rules French Court' (The Daily Mail 2010) <http://www.dailymail.co.uk/news/worldnews/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html> accessed April 2011)

M Ward, 'China's Tight Rein on Online Growth' (British Broadcasting Corporation 2005) <http://news.bbc.co.uk/1/hi/technology/4327067.stm> accessed April 2011

YLE, '1Mb Broadband Access Becomes Legal Right' (Finnish Broadcasting Company 2009) http://www.yle.fi/uutiset/news/2009/10/1mb_broadband_access_becomes_legal_right_1080940.html accessed April 2011)