

CLAIM NO.

IN THE HIGH COURT OF JUSTICE

ADMINISTRATIVE COURT

BETWEEN

THE QUEEN

ON THE APPLICATION OF

(1) BRITISH TELECOMMUNICATIONS PLC

(2) TALKTALK TELECOM GROUP PLC

Claimants

-and-

THE SECRETARY OF STATE FOR BUSINESS, INNOVATION AND SKILLS

Defendant

STATEMENT OF FACTS AND GROUNDS

A. Introduction

1. The First Claimant ('BT') is a public limited company incorporated under the laws of England and Wales. The Second Claimant ('TTG') is also a public limited company incorporated in England. Each carries on business in the supply of telecommunications services and equipment to both businesses and residential customers. Both BT and TTG are also internet service providers ('ISPs').
2. The Defendant ('the Secretary of State') is the Government minister designated with responsibility for the Department of Business, Innovation and Skills ('DBIS').
3. The Claimants seek permission to apply for judicial review of the provisions of the Digital Economy Act 2010 (c. 20) governing Online infringement of copyright (sections 3 to 18) ('the contested provisions'). The Act received Royal Assent on 8 April 2010.
4. The essential reading in support of this application is:

- 4.1. The witness statement of Simon Milner on behalf of BT dated 5 July 2010;
 - 4.2. The witness statement of Andrew Heaney on behalf of TTG dated 5 July 2010;
 - 4.3. The experts' report of Professor Robin Mansell of the London School of Economics and Professor Edward Steinmueller of the University of Sussex dated 1 July 2010;
 - 4.4. The Explanatory Notes to the Digital Economy Bill at Exhibit SM-12, in particular paragraphs 35, 36, 39, 47, 48, 51, 52 and 59;
 - 4.5. The Impact Assessment and Revised Impact Assessment, at Exhibits SM-13 and SM-14, in particular at pages 91 to 123 of the internal report of SM-14;
 - 4.6. The draft Initial Obligations Code issued by Ofcom in May 2010 at Exhibit SM-23.
5. The time estimate for this reading is six hours.

B. Summary of the Claimants' case

6. The Claimants are concerned that the contested provisions of the DEA 2010 represent a disproportionate response to the concerns identified by the Secretary of State concerning unlawful peer-to-peer file sharing. As is apparent from the witness evidence and experts' report served in this case, the contested provisions of the DEA 2010 are likely to have a significant impact on internet users, many of whom are likely to be wholly unconnected with any form of digital piracy on a commercial scale. The requirements imposed by the DEA 2010 raise very serious concerns about the impact on the privacy of internet users and the confidentiality expected by subscribers in their dealings with BT, TTG and other ISPs.
7. The DEA 2010 requires the Claimants to set up and administer costly schemes in relation to the internet use of their subscribers, to amend substantially their existing data processing practices and to incur potential liability to their subscribers as a result of their actions. The Claimants are also disconcerted at the prospect of their being required to discharge an enforcement function on behalf of copyright owners in circumstances where no, or no adequate, provision has been made for the costs of doing so. The Claimants have already had to incur significant costs in preparation for the full entry into force of the DEA 2010 and the obligations imposed by the contested provisions.

8. The Claimants contend that the contested provisions of the DEA 2010 are unlawful as a matter of EU law. They are anxious to ensure that all concerns about the validity of the provisions are resolved before the due date for full implementation of the regime arises. It is important for the Claimants (and for subscribers) that any concerns about the legality of the contested provisions are resolved before even more substantial costs are incurred and before individual appeals might be brought by subscribers against the actions of either copyright owners or ISPs. In addition, if there is uncertainty about the legality of the provisions and some ISPs decide to ignore the provisions or challenge their legality at a later date, this could have obvious and adverse commercial repercussions for those ISPs who have incurred substantial costs complying with the contested provisions of the DEA 2010 from the outset. It would also have a distortive effect on competition within the market.
9. The Claimants consider that a responsible reaction to these concerns is to seek declaratory relief from this Court, so that the legality of the contested provisions can be the subject of authoritative judicial pronouncement.
10. The Claimants contend that the contested provisions are incompatible with EU law for all or some of the following reasons:
 - 10.1. The contested provisions constitute a technical regulation and/or a rule on services within the meaning of the Technical Standards Directive.¹ They should have been notified to the EU Commission, but have not been. The provisions are accordingly unenforceable;
 - 10.2. The contested provisions are incompatible with the Electronic Commerce Directive ('the E-Commerce Directive');²
 - 10.3. The contested provisions are incompatible with the Privacy and Electronic Communications Directive ('the PEC Directive') and with the requirement that the measures in issue should be proportionate;³

¹ 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, p. 37, 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, p. 18.

² 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, p. 1.

10.4. Further or alternatively, the contested provisions are disproportionate in their impact on ISPs, business and consumers. They accordingly infringe:

10.4.1. Article 56 TFEU (ex Article 49 EC) coupled with Article 61 TFEU (ex Article 55 EC) and Article 52 TFEU (ex Article 46 EC), as a disproportionate restriction on the ability of internet services providers to provide internet services in the United Kingdom;

10.4.2. Article 3(4) of the E Commerce Directive;

10.4.3. Article 15(1) of the PEC Directive;

10.4.4. Articles 8 and/or 10 of the European Convention on Human Rights, as given effect to through:

10.4.4.1. Article 6(3) TEU;

10.4.4.2. General principles of Union law;

10.4.4.3. The requirements of the Framework Directive, as amended⁴;

10.4.4.4. Equivalent rights conferred by Articles 7, 8, 11 and 52 of the Charter of Fundamental Rights of the European Union and Article 6(1) TEU;⁵ and/or

10.4.4.5. The Human Rights Act 1998.

11. The Claimants seek the following relief:

11.1. A quashing order in respect of sections 3 to 18 of the DEA 2010;

11.2. Alternatively, declaratory relief to the effect that the contested provisions are unlawful for all or some of the reasons set out in paragraph 10 above;

11.3. Costs.

C. Factual Background

12. There is attached to this Statement of Facts and Grounds a short chronology setting out the key events to date. In addition, a detailed summary of the history behind the Digital

³ 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 p. 37.

⁴ Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/12/EC on a common regulatory framework for electronic communications, networks and services, 2002/19/EC on access to, and interconnection of, electronic communications, networks and associated facilities, and 2002/20/EC on the authorization of electronic communications, networks and services, OJ [2009] L No 337, p. 37.

⁵ OJ [2000] C No. 364, p. 1.

Economy Act 2010 can be found in the witness statement of Simon Milner on behalf of BT, dated 5 July 2010.

(1) The framework within which ISPs operate

13. The liberalisation of the telecommunications sector has been achieved through the privatisation of a number of former state monopolies in different Member States of the European Union. The EU has been very active in promulgating a series of measures designed to achieve a consistent regulatory approach between telecoms providers in different Member States. The measures of particular relevance to the Claimants' business are:

- 13.1. the Framework Directive;⁶
- 13.2. the Authorisation Directive;⁷
- 13.3. the Access Directive;⁸
- 13.4. the Universal Service Directive;⁹
- 13.5. the PEC Directive.¹⁰

14. These five key directives set out the major provisions governing the “telecoms package” introduced by the EU to harmonise the cross-border provision of telecommunications services in the EU. These core five Directives have also been augmented by :

- 14.1. The provisions of the Radio Spectrum Decision;¹¹
- 14.2. The Competition Directive;¹²

⁶ European Parliament and EC Council Directive 2002/21 (OJ L108, 24.4.2002, p 33) on a common regulatory framework for electronic communications networks and services (amended by European Parliament and EC Council Regulation 717/2007 (OJ L171, 29.6.2007, p 32); European Parliament and EC Council Regulation 544/2009 (OJ L167, 29.6.2009, p 12); and European Parliament and EC Council Directive 2009/140 (OJ L337, 18.12.2009, p 37)).

⁷ European Parliament and EC Council Directive 2002/20 (OJ L108, 24.4.2002, p 21) on the authorisation of electronic communications networks and services (amended by European Parliament and EC Council Directive 2009/140 (OJ L337, 18.12.2009, p 37)).

⁸ European Parliament and EC Council Directive 2002/19 (OJ L108, 24.4.2002, p 7) on access to, and interconnection of, electronic communications networks and associated facilities (amended by European Parliament and EC Council Directive 2009/140 (OJ L337, 18.12.2009, p 37)).

⁹ European Parliament and EC Council Directive 2002/22 (OJ L108, 24.4.2002, p 51) on universal service and users' rights relating to electronic communications networks and services (amended by European Parliament and EC Council Directive 2009/136 (OJ L337, 18.12.2009, p 11)).

¹⁰ European Parliament and EC Council Directive 2002/58 (OJ L201, 31.7.2002, p 37) concerning the processing of personal data and the protection of privacy in the electronic communications sector (amended by European Parliament and EC Council Directive 2006/24 (OJ L105, 13.4.2006, p 54); and European Parliament and EC Council Directive 2009/136 (OJ L337, 18.12.2009, p 11)).

¹¹ European Parliament and EC Council Decision 676/2002 (OJ L108, 24.4.2002, p 1) on a regulatory framework for radio spectrum policy in the European Union.

- 14.3. The Directive on competition in the markets in telecommunications terminal equipment;¹³
 - 14.4. The Regulation on unbundled access to the local loop;¹⁴
 - 14.5. The Regulation on roaming on public mobile telephone networks within the Community;¹⁵ and
 - 14.6. The Regulation establishing the Body of European Regulators for Electronic Communications ('BEREC') and the Office.¹⁶
15. The Office of Communications Act 2002 and the Communications Act 2003 ('CA 2003') launched a major re-organisation of telecommunications markets domestically in the United Kingdom, under the regulatory control of Ofcom.
16. The result of this legislation has been a highly co-ordinated approach to regulation of telecoms providers on a pan-European level since 2002. The regulation at both an EU and a national level has been designed to promote competition between telecoms providers and protect consumer interests, while ensuring that a universal service is available for the majority of telecommunications services (access to landline telephony, mobile phone telephony and internet access). A universal service obligation is proposed in respect of broadband access for consumers.
17. Numerous obligations have been implemented requiring ISPs not to interfere with the privacy of subscribers' use of the internet or monitor traffic and to respect their confidentiality. Article 5 of the PEC Directive requires Member States to ensure that the confidentiality of communications and related traffic data by means of a public communications network is respected under national legislation. Domestic legislation must prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data by persons other than users, without either: (a)

¹² Commission Directive 2002/77 (OJ L249, 17.9.2002, p 21) on competition in the markets for electronic communications networks and services.

¹³ Commission Directive 2008/63 (OJ L162, 21.6.2008, p 20) on competition in the markets in telecommunications terminal equipment.

¹⁴ European Parliament and EC Council Regulation 2887/2000 (OJ L336, 30.12.2000, p 4) on unbundled access to the local loop.

¹⁵ European Parliament and EC Council Regulation 717/2007 (OJ L171, 29.6.2007, p 32) on roaming on public mobile telephone networks within the Community and amending Directive 2002/21/EC (amended by European Parliament and EC Council Regulation 544/2009 (OJ L16, 29.6.2009, p 12)).

¹⁶ European Parliament and EC Council Regulation 1211/2009 (OJ L337, 18.12.2009, p 1) establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office.

the consent of the user; or (b) a legally permissible authorisation to do so under Article 15 of that Directive. This requirement is expressed not to prevent technical storage of data which is necessary for the conveyance of a communication, while protecting its confidentiality. In addition, Article 5(2) permits the legal authorisation of recording of communications and related traffic data carried out in the course of lawful business activity.

18. In addition, Article 6 of the PEC Directive imposes a general requirement for traffic data¹⁷ relating to subscribers or users which is processed and stored by a public communications provider to be erased or made anonymous when no longer required for the purpose of the transmission of a communication.

19. Article 6(5) of the PEC Directive circumscribes the circumstances under which traffic data may be processed by BT or TTG. Traffic data relating to a subscriber or user may be processed and stored by a provider of a public electronic communications service if:

19.1. such processing and storage are for the purpose of marketing electronic communications services, or for the provision of value added services to that subscriber or user; and

19.2. the subscriber or user to whom the traffic data relates has given his consent to such processing or storage; and

19.3. such processing and storage are undertaken only for the duration necessary for the purposes specified.

20. The overall regime recognises the neutral and essentially passive role played by ISPs. ISPs do not have control over the use to which their services are put, but are mere “conduits” for the communications data conveyed over the internet. The telecoms package also imposes restrictions on the extent to which ISPs may lawfully process or retain the content of electronic communications or details about their transmission. This passive role has been recognised by the Courts at common law, in such areas as defamation. See, for example, Metropolitan International Schools v. Design Technica Corporation and Google UK Ltd [2009] EWHC 1765 (QB), [2009] EMLR 27, per Eady J. A similar exception to liability for copyright infringement is provided in Article 5 of

¹⁷ Traffic data is defined in Article 2(b) of the Privacy Directive as “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.”

the Directive of the European Parliament and of the Council Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society ('the Copyright Directive').¹⁸ That enables "temporary acts of reproduction . . . which are transient or incidental, which are an integral and essential part of a technical process and whose sole purpose is to enable – (a) a transmission in a network between third parties by an intermediary."

(2) *The Memorandum of Understanding*

21. The growth of broadband access to the internet has had a dramatic effect on the provision of online services. Access to digital material in all forms has become significantly easier and quicker as "download" and "upload" speeds have increased. A thriving internet market has developed, through which a variety of digital material may be sold by businesses and purchased by other businesses or consumers.
22. Software developers have created file-sharing software enabling an internet user on one computer to access files and material stored on another user's computer where the second user is also connected to the internet. This software may be used for many different purposes, such as sharing photographs between family and friends and transferring digital media files between a desktop and a laptop computer owned by the same individual or family. In addition, as the fact sheets produced by DBIS make clear (Exhibit SM-15), file-sharing software has many legitimate commercial uses: for example, Linux "open source" software is based on P2P file-sharing. Companies such as Facebook use it to update software used for their services. Companies in the entertainment industry are increasingly using it to distribute their works to users. The music streaming service Spotify is also based on the software. Academic and research institutions use it to send very large files. The Government has stated that it does not wish to interfere with this legitimate use of technology.
23. The Government, however, has stated that there has been an increase in the unlawful transfer of digital media material between users in breach of the copyright protection attaching to such material. Examples of such unlawful use include, at one end of the

¹⁸ OJ [2001] L No. 167, p. 10.

spectrum, teenagers swapping music files between each other to sample each other's taste in music. At the other end, the file-sharing may amount to a commercial or quasi-commercial distribution of pirated music, videos, games or software.

24. A detailed description of how file-sharing software works has been given in fact sheets prepared by DBIS in December 2009 (at Exhibit SM-15):

“How does it work?”

The software typically used in file-sharing was developed in order to allow people to make the most effective use of computer networks. Rather than relying on a central file server (people going to a common source which holds millions of files in one place), a P2P computer network has no central store of files. Instead, it uses a series of ad hoc connections between participants in a network and the cumulative bandwidth of network participants. This first took the form of a central file server which acted as “index” and introduced two users together (one with the content; the other seeking the content). This was the original “Napster” model (diagram 1). Later, the need for a central index was dropped and P2P networks became de-centralised (diagram 2). Such networks are used for many purposes - sharing files (i.e. file-sharing) containing audio, video, data or anything in digital format is very common, and real-time data, such as telephony traffic, is also passed using P2P technology.

The advantage of a P2P network is that all users provide resources, including bandwidth, storage space, and computing power. As additional users arrive, and demand on the system increases, the total capacity of the system also increases. This is not the same for client-server architecture with a fixed set of servers, where adding more clients could mean slower data transfer for all users. As there is no one central server, P2P networks are typically more robust. Furthermore, as individuals use a number of different connections to download the (same) information, this avoids bottlenecks.

Many of the most popular file-sharing sites (such as Limewire) use BitTorrentTM technology. This is a protocol (a set of rules and a description of how to do things) which allows users to download files by allowing those downloading the file to upload parts of it at the same time. It therefore works by downloading small bits of files from many different web sources at the same time.

A key feature of P2P file-sharing software commonly used in illicit file-sharing is that in order to participate and download files, the user is expected to make available the files on their computer. In other words, if you want to copy files from someone, then your own files should be equally available for others to copy. It is such reciprocal arrangements that enable P2P in illicit copyright to happen on the scale it does. (*sic*)”

25. The fact sheet also describes how copyright holders are able to detect that their copyright material has been unlawfully transferred:

“How do copyright owners detect copyright infringements?”

It is also this feature which allows the rights holders to identify who is unlawfully copying material. The act of joining a P2P network and actively accessing copyrighted material for download provides them with the IP address of the up-loader. In order to take legal action against [an] infringer uploading these files the rights holder needs to relate this IP address to an account holder and a physical UK address – the computer records held by the ISP can provide this information, and is obtainable via a court order. Under the Digital Economy Bill, this will not change – except that the Bill will enable rights holders to identify those account holders who have been identified by them as infringing most often (which they would not know from the IP address alone, since this is generally dynamic – it changes each time you log on).

It is not difficult to identify which Internet Service Provider (ISP) is responsible for the IP address (lists of who holds what batches of addresses are readily obtainable), and so this is not something that should exclude smaller rights holder organisations from entering the process. Under the provisions in the Bill, they will have to comply with the standard of evidence to be set out by the code, and to pay the flat fee for sending the notification, plus a share of the regulator’s costs.

...

Why is the uploader the focus of the approach?

The way in which copyright owners find out about online copyright infringement is to go on-line and search for their material. As they know who is entitled to offer their content, they are able to identify unauthorised sources – this is the uploader. By downloading material from the uploader they are able to establish that it is their material and thereby gain evidence which can be used to identify the uploader. For the data transfer – the copying – to take place the uploader and downloader reveal their IP address to the other.

The only way to identify the downloader would be to offer material for copying (i.e. become the uploader). However, in doing so the copyright owner is arguably inciting such actions.”

26. In order to combat the alleged increase in unlawful file-sharing, BT, TTG and other ISPs were strongly encouraged by the Government to endorse a Memorandum of Understanding with the British Phonographic Industry (‘BPI’) and other rights owners in July 2008 (Exhibit SM-1 at Annex D). ISPs undertook to work together with other signatories on a process whereby internet service customers were informed when their accounts were being used unlawfully to share copyright material and pointed towards legal alternatives. The Claimants participated in a three month trial to send notifications to subscribers identified to them by music rights holders, as having been engaged in illicit uploading or downloading.

27. The MOU was part of a multi-pronged approach to the problem of unlawful P2P file-sharing. It also encouraged co-operation between relevant industries, education of the consumer, improved availability of online content and consideration of better business models for content delivery, as well as notifications to customers and steps suggested for

dealing with persistent infringers. A combined Principle 2 and Principle 3 Working Group was set up under the MOU to report on commercial solutions to what the Claimants saw as a market problem. The MOU three-month trial period expired in January 2009.

(3) *Digital Britain: The Interim Report*

28. In January 2009, the Department for Culture, Media and Sport ('DCMS') and the Department for Business, Enterprise and Regulatory Reform ('DBERR'), now known as the Department for Business, Innovation and Skills ('DBIS'), published a paper entitled *Digital Britain: Interim Report* (Cm 7548). A copy is at Exhibit SM-5. The paper proposed the enactment of legislation which would require ISPs to notify alleged infringers of rights that their conduct is unlawful (upon the supply of reasonable proof by rights-holders); coupled with a requirement on ISPs to collect 'anonymised' information on serious repeat infringers which could be made available to rights-holders upon production of a Court order.

(4) *The Government White Paper*

29. In June 2009, the Government published its White Paper on Digital Britain, entitled *Digital Britain: Final Report* (Cm 7650). It can be found at Exhibit SM-6. This set out a series of Government proposals designed to put the United Kingdom at the forefront of "the global move towards a digital knowledge economy." The Government as part of this aim set out to control unlawful peer-to-peer file sharing.

30. The White Paper endorsed the approach that had been articulated in the Interim Report, namely the requirement for ISPs to comply with the twin requirements of notifying subscribers of infringements passed to them by copyright holders and of maintaining 'anonymised' lists of repeats offenders (the identity of whom could be made subject to a request for disclosure by the copyright holders by Court order).

31. In addition, the White Paper raised the possibility of further legislative measures being adopted if the "initial obligations" did not produce the desired reduction in unlawful file-sharing. The envisaged measures included:

- 31.1. The blocking of access to websites, internet protocol ('IP') addresses or to a uniform resource locator (or URL, which is the global address of documents and other resources on the worldwide web);
 - 31.2. Protocol blocking (preventing certain internet protocols from accessing the internet which can prevent certain internet services being used by a computer);
 - 31.3. Port blocking (preventing certain ports from accessing the internet, with the same aim as protocol blocking);
 - 31.4. Bandwidth capping (which reduces the speed at which files might be downloaded);
 - 31.5. Volume capping (restricting the amount of data that may be downloaded over a period of time);
 - 31.6. Bandwidth shaping (limiting the speed of a subscriber's access to selected protocols or services);
 - 31.7. Content identification and filtering.
32. The Government's proposal was to spell out the detail of these various obligations in a Code which was either to be industry made and approved by Ofcom, or made by Ofcom itself.

(5) The Digital Economy Bill

33. The Government thereafter conducted a consultation exercise. In the course of this exercise, it raised various options concerning the degree of costs-sharing between rights holders and the ISPs regarding the cost of complying with the initial obligations.
34. The Government published its response to the consultation exercise in November 2009 (Exhibit SM-10). It announced that legislation to tackle online copyright infringement would be introduced in the Digital Economy Bill. In keeping with its previous stance, the Government indicated that the Bill would introduce two "straightforward obligations", whose detailed practical implementation would be left to be spelled out in an industry approved Code (or in default by Ofcom). The costs proposals previously advanced were replaced by a proposed "flat fee" system, by which rights owners paid an ISP a flat fee for processing each of its "copyright infringement reports" ('CIRs').

35. On 16 November 2009, the Government published the Digital Economy Bill. It was introduced to the Houses of Lords on 19 November 2009 (Exhibit SM-11). Paragraph 8 of the Explanatory Notes (Exhibit SM-12) stated that:

“Topic 2 is online infringement of copyright. Clauses 4 to 17 impose on internet service providers obligations aimed at the reduction of online infringement of copyright. OFCOM is responsible for the specification of the procedural and enforcement aspects of these obligations through the approval or adoption of legally binding codes of practice. Clause 17 gives power to the Secretary of State to make provision by order to amend Part 1 or Part 7 of the Copyright Designs and Patents Act 1988 for the purpose of preventing or reducing on-line copyright infringement.”

36. Paragraph 34 of the Explanatory Notes accompanying the Bill indicated that:

“The provision inserts new sections 124A to 124M in the Communications Act 2003 (“the 2003 Act”), **which impose obligations on internet service providers (“ISPs”)** to:

- Notify their subscribers if the internet protocol (“IP”) addresses associated with them are reported by copyright owners as being used to infringe copyright; and
- Keep track of the number of reports about each subscriber, and compile, on an anonymous basis, a list of some or all of those who are reported on. After obtaining a court order to obtain personal details, copyright owners will be able to take action against those included in the list.” [Emphasis added]

37. Paragraph 35 confirmed that these obligations would be underpinned by a code approved by Ofcom or, if no industry code was put forward for approval, a code made by Ofcom. The Explanatory Notes stated that the Code would “set out in detail how the obligations must be met.”

38. Furthermore, paragraph 36 observed that the structure of the Bill was such that if the initial obligations imposed did not achieve the objective of reducing unlawful file-sharing to a satisfactory extent, then additional “technical obligations” would be imposed on ISPs. These would require ISPs to limit internet access to certain subscribers, for example through bandwidth capping or shaping, or through temporary suspension in certain circumstances.

39. Paragraph 39 recognised that provision would have to be made for apportionment of the costs of operating a notification system. Paragraph 39 itself set out an illustrative example of how the obligations might take shape in practice:

“To illustrate how the provisions might work in practice, possible processes of notification and court action are outlined below:

- Copyright owners identify cases of infringement and send details including IP addresses to ISPs;
- The ISPs verify that the evidence received meets the required standard, and link the infringement to subscriber accounts;
- The ISPs send letters to subscribers identified as apparently infringing copyright. They keep track of how often each subscriber is identified;
- If asked to do so by a relevant copyright owner, ISPs supply a serious infringers list showing, for each subscriber who has been identified repeatedly by the copyright owner, which of the copyright owner’s reports relate to that subscriber. The list does not reveal any subscriber’s identity;
- Copyright owners use the serious infringers list as the basis for a large scale “Norwich Pharmacal” court order to obtain the names and addresses of some or all of those on the list. At no point are individuals’ names or addresses passed from the ISP to a copyright owner without a court order;
- Copyright owners send “final warning” letters direct to infringers asking them to stop online copyright infringement and giving them a clear warning of likely court action if the warning is ignored; and
- Copyright owners take court action against those who ignore the final warning.”

40. In terms of the two initial obligations imposed on ISPs, paragraph 47 of the Explanatory Notes described the imposition of the first obligation under Clause 4 in the following terms:

“The notification from the ISP must inform the subscriber that the account appears to have been used to infringe copyright, and it must provide evidence of the apparent infringement, direct the consumer towards legal sources of content, and provide other advice.”

41. Paragraph 48 gave the following explanation of the content of the obligation found in Clause 5:

“ISPs will have to keep a record of the number of CIRs linked to each subscriber along with a record of which copyright owner sent the report. Under section 124B of the 2003 Act, inserted by clause 5, an ISP may be required to provide a copyright owner with relevant parts of those records on request (“copyright infringement lists”), but in an anonymised form so as to ensure compliance with data protection legislation.”

42. Paragraphs 51 and 52 of the Explanatory Notes stated that the obligations in the proposed Act would not take formal effect until a Code was published. The Code would deal with the “points of detail.” The Government’s stated intention (at paragraph 55) was for the

obligations imposed by the Bill to fall on all ISPs except those who are demonstrated to have a very low level of online infringement.

43. The contents of the “initial obligations code” were addressed in Clause 8 of the Bill and paragraph 59 of the Explanatory Notes. A proposed section 124E of the Communications Act 2003 would set out what the Code must contain in terms of a minimum set of obligations to be imposed on ISPs. The stated reason for setting the fuller details down in the Code was that the specific obligations and procedures would be detailed and were likely to have to be adapted over time.

(6) The impact assessment for the Digital Economy Bill

44. The Bill was the subject of a regulatory Impact Assessment issued in November 2009 (Exhibit SM-13). It was updated in March 2010 following some amendments to the Bill during its passage through the House of Lords (Exhibit SM-14).

45. The updated Assessment made *inter alia* the following findings:

45.1. The average annual costs of compliance by ISPs were put at £30 to £50 million a year;

45.2. The average annual benefit to rights holders in displaced sales was £200 million;

45.3. The net benefit using net present values for the assessment was £1.2 billion to £1.4 billion;

45.4. The costs to digital product consumers were not taken into account, since the content was said only to be available illegally. Furthermore, effects on the poorest consumers, who would cease consumption of digital content altogether, were not taken into account, since the assumption was made that such consumers would only be consuming material illegally. US studies had indicated that the total welfare loss to consumers as a whole would be twice that of the estimated displaced revenues to the digital industry;

45.5. There were uncertainties about the estimate of the sales displacement figure for rights holders and other costs;

- 45.6. A number of studies had in fact found that the displacement effect of P2P downloading was zero. If that were right, the costs of implementing legislation would vastly outweigh the benefits, which would be negligible. The two studies which had reached this conclusion identified in Table 1 at page 107 were studies that had been based on actual downloads data, rather than surveys or download proxies data;
- 45.7. The estimated one off costs to ISPs of the scheme would be in the region of £20 million to £65 million. Annual average costs thereafter were likely to be in the region of £7.5 million to £24.5 million. But compliance costs were very sensitive to the underlying assumptions that lay behind them;
- 45.8. It was considered that the average one off costs for the 5 largest ISPs in the UK (which include BT and TTG) would be £3m to £10m. The average annual costs thereafter would be between £1m and £3m.
- 45.9. An additional administrative burden of operating the databases needed to store details of infringers was estimated at £6.9m to £22.6m per year;
- 45.10. Further costs of £200,000 as a one-off cost and annual costs of £65,000 per annum would be needed for call centres;
- 45.11. A range of values was also assigned to capital costs, depending on the method of implementation adopted by the ISPs;
- 45.12. The predicted effect on ISP lost revenue was assessed to be between £2m and £9m per annum;

46. The Assessment did not assess many costs that would result from the obligations including *inter alia* the level of cost, inconvenience or distress caused to subscribers who were wrongly identified as infringers, full administration costs, harm and losses resulting from technical obligations and competitive distortion. For example, at internal pages 112-113, the Assessment commented that:

“Scenario Three

There are about 20 operators who run are also wholesale providers (*sic*); this includes the 5 largest ISPs. It may be the case broadband resellers, who rebrand and sell the services offered by the wholesale providers, need not invest because the wholesale providers do so on their behalf. It is difficult to say how many wholesale providers would automate and process CIRs on behalf of the smaller ISPs; therefore it is assumed that all 20 do so as not to underestimate the costs. If this is the case the costs to ISPs of investing would be £1.6million.

ISPs have indicated that there would be further costs derived from keeping the records of infringers as requested by the proposed legislation. It is not possible to provide an estimate of such expenditures at this time.

Identification of infringers is technically more complex for mobile network operators. A single customer does not use a unique IP address as in fixed broadband networks. Instead, an IP address is shared by multiple costumers, therefore making it very difficult to distinguish the real infringers from the rest of users. Additionally, in order to identify infringers mobile network operators must monitor all the data activities undertaken by their subscribers. This implies that the costs are going to be necessarily higher and that there could also be data protection implications.

47. The Digital Economy Bill received Royal Assent on 8 April 2010.

D. The Digital Economy Act 2010

48. Given that the Claimants seek to challenge the contested provisions of the DEA 2010, the material parts of it are set out in full in an Annex to this Statement of Facts and Grounds.

E. Grounds of Review

49. BT and TTG advance four heads of challenge to the contested provisions of the DEA 2010. They are:

- 49.1. The contested provisions contravene the requirements of the Technical Standards Directive;
- 49.2. The contested provisions are incompatible with the E Commerce Directive;
- 49.3. The contested provisions are incompatible with the PEC Directive;
- 49.4. The contested provisions are disproportionate in their effect, in that they unduly restrict the ability of ISPs established in other Member States to provide internet services in the United Kingdom and/or infringe Articles 8 and/or 10 of the European Convention on Human Rights and equivalent provisions found in the EU Charter on Fundamental Rights.

50. The heads of challenge will be addressed in turn.

(1) Ground 1: Contravention of the Technical Standards Directive

51. The contested provisions of the DEA 2010 should have been notified to the EU Commission under the relevant provisions of 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 and of rules on Information Society services ('the Technical Standards Directive').¹⁹ They were not so notified. In the absence of notification, the contested provisions are unenforceable.

(a) The relevant legal provisions

52. The original Technical Standards Directive was substantially amended and extended by Directive 98/48/EC. The purpose of the amendment, as revealed by Recital (1) to Directive 98/48/EC was "to promote the smooth functioning of the internal market", by providing for "as much transparency as possible . . . as regards the future national rules and regulations applying to Information Society services." Recital (8) provided the following warning:

"Whereas without coordination at Community level, this foreseeable regulatory activity at national level might give rise to restrictions on the free movement of services and the freedom of establishment, leading in turn to a refragmentation of the internal market, over-regulation and regulatory inconsistencies."

53. Recital (9) accordingly recognised the need for a co-ordinated approach in this eminently transnational area. Recital (12) recorded that:

"(12) Whereas it is therefore necessary to preserve the smooth functioning of the internal market and to avert the risks of refragmentation by providing for a procedure for the provision of information, the holding of consultations, and administrative cooperation in respect of new draft rules and regulations; whereas such a procedure will help, inter alia, to ensure that the Treaty, in particular Articles 52 and 59 thereof, is effectively applied and, where necessary, to detect any need to protect the general interest at Community level; whereas, moreover, the improved application of the Treaty made possible by such an information procedure will have the effect of reducing the need for Community rules to what is strictly necessary and proportional in the light of the internal market and the protection of general-interest objectives; whereas, lastly, such a procedure will enable businesses to exploit the advantages of the internal market more effectively;"

¹⁹ See footnote 1 above.

54. The EU legislature accordingly recognised that the framework of “administrative co-operation” (falling short of actual harmonisation measures) provided by the Technical Standards Directive could be extended so as to ensure that Information Society services could be provided between Member States of the EU on a level playing field. Recital (16) to Directive 98/48/EC stated that:

“(16) Whereas notification should be provided for notably in the case of rules which are likely to evolve in future; whereas services which are provided at a distance, electronically, and at the individual request of a recipient of services (Information Society services) are likely, in view of their diversity and their future growth, to necessitate and generate the largest number of new rules and regulations; **whereas provision must accordingly be made for the notification of draft rules and regulations relating to such services.**” [Emphasis added]

55. Recital (17) also noted that “specific rules” on the taking-up and pursuit of service activities which are capable of being carried on in the manner described above should be communicated to the Commission, even where they are included in rules and regulations with a more general purpose. Nonetheless, “general regulations **which do not contain any provision specifically aimed at such services** need not be notified.” [Emphasis added]

56. Recital (18) gives guidance on the sort of services which would and would not be covered by the expression “Information Society service.”

“Whereas ‘rules on the taking-up and pursuit of service activities’ means rules laying down requirements concerning Information Society services, such as those relating to service providers, services and recipients of services and to economic activities capable of being provided electronically, at a distance and at the individual request of the recipient of the services; whereas, for example, rules on the establishment of service providers, in particular those on authorisation or licensing arrangements, are accordingly covered; **whereas a provision specifically aimed at Information Society services must be considered as being such a rule even if part of a more general regulation;** whereas, on the other hand, measures of direct and individual concern to certain specific recipients (such as, for example, telecommunications licences) would not be covered.” [Emphasis added]

57. Information Society Service is defined in Article 1(2) of the Amended Directive 98/34/EC.

“‘service’, any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:

- ‘at a distance’ means that the service is provided without the parties being simultaneously present,
- ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.”

58. Directive 98/48/EC also introduced the concept of a “rule on services” which would in principle be treated as the functional equivalent to a “technical regulation” for the purposes of Directive 98/34/EC. The definition provided in the amended Article 1(5) is as follows:

“5. ‘rule on services’, requirement of a general nature relating to the taking-up and pursuit of service activities within the meaning of point 2, in **particular provisions concerning the service provider, the services and the recipient of services, excluding any rules which are not specifically aimed at the services defined in that point.**

...

For the purposes of this definition:

- a rule shall be considered to be specifically aimed at Information Society services where, having regard to its statement of reasons and its operative part, **the specific aim and object of all or some of its individual provisions is to regulate such services in an explicit and targeted manner,**
- a rule shall not be considered to be specifically aimed at Information Society services if it affects such services only in an implicit or incidental manner.” [Emphasis added]

59. The relevant definition of technical regulation provided by Article 1(11) is now as follows:

“‘technical regulation’, technical specifications and other requirements or rules on services, including the relevant administrative provisions, the observance of which is compulsory, *de jure* or *de facto*, in the case of marketing, provision of a service, establishment of a service operator or use in a Member State or a major part thereof, as well as laws, regulations or administrative provisions of Member States, except those provided for in Article 10, prohibiting the manufacture, importation, marketing or use of a product or prohibiting the provision or use of a service, or establishment as a service provider.

De facto technical regulations include:

- **laws, regulations or administrative provisions of a Member State** which refer either to **technical specifications or to other requirements or to rules on services**, or to professional codes or codes of practice which in turn refer to technical specifications or to other requirements or to rules on services, compliance with which confers a presumption of conformity with the obligations imposed by the aforementioned laws, regulations or administrative provisions, . . .” [Emphasis added]

60. Article 1(12) now defines a draft technical Regulation as follows:

“‘draft technical regulation’, the text of a technical specification or other requirement **or of a rule on services**, including administrative provisions, formulated with the aim of enacting it or of ultimately having it enacted as a technical regulation, **the text being at a stage of preparation at which substantial amendments can still be made.**” [Emphasis added]

61. It follows that a rule on services (as defined) is included within the definition of a technical regulation or a draft technical regulation, as the case may be.

62. In order to place the substantive obligations imposed by the Technical Standards Directive in context, it is appropriate also to consider the recitals to the unamended version of Directive 98/34/EC. In this regard:

62.1. The purpose behind the Technical Standards Directive is to promote the smooth functioning of the internal market and to require as great a degree of transparency as possible to national initiatives for the establishment of technical standards. See recital (3);

62.2. The EU’s concern is to ensure that technical regulations are strictly necessary in the public interest and do not constitute undue barriers to trade: recital (4);

62.3. The Commission must have the necessary information on national technical standards before it and so an obligation to notify it is imposed on Member States in respect of their “projects in the field of technical regulations.” The notification provision will also enable other Member States and other commercial operators to be put in the picture. See recitals (5) to (7);

62.4. The notification mechanism also enables the Commission and other Member States to propose amendments to a contemplated measure: recital (13);

62.5. The standstill provision also enables the Commission and Member States to consider whether legislative action is better taken at an EU level: recitals (15) and (16).

63. Pursuant to Article 8(1) of the Technical Standards Directive, the United Kingdom is obliged to communicate immediately to the Commission any draft technical regulation, except where it merely transposes the full text of an international or European standard. In so communicating, the UK is also obliged to issue a statement of the grounds on which such a technical regulation is necessary, in so far as they are not clear from the draft. Member States are also obliged to communicate the draft again “if they make changes to the draft that have the effect of significantly altering its scope, shortening the timetable originally envisaged for implementation, adding specifications or requirements, or making the latter more restrictive.”

64. Article 8(2) then envisages that the Commission and Member States may pass comments on the draft technical regulation to the Member State issuing it, which that Member State will then take into account. Article 8(3) imposes an obligation on Member States to communicate the text of the definitive Regulation.

65. Article 9(1) of the Directive imposes a “standstill” requirement on Member States to postpone the adoption of a draft technical regulation for a period of three months from the date of communication. This is to give the Commission, other Member States and other commercial operators time to consider it.

66. Article 9(2) now provides that in the case of a rule on services, Member States shall, subject to Articles 9(4) or 9(5), operate the “standstill” for an extended period of four months from the date of communication, if the Commission or another Member State delivers a detailed opinion, within three months of that date, to the effect that the measure envisaged may create obstacles to the free movement of services or to the freedom of establishment of service operators within the internal market.²⁰

²⁰ See Case C-42/07 Liga Portuguesa de Futebol Profissional v. Departamento de Jogos [2009] ECR I-0000, [2010] 1 CMLR 1, ECJ per Advocate General Bot at [53]: “Therefore Directive 98/34 provides for a system whereby each Member State must notify the Commission of its proposed technical regulations so as to enable the Commission and the other Member States to inform it of their viewpoint and to propose a standardisation

67. The effect of these provisions is that the Commission and/or Member States have a period of three months from the communication of the measure to raise an objection to it on free movement grounds. If an objection is raised within that period, an additional standstill of a month is imposed.
68. In addition, the Member State is obliged to postpone adoption for a period of 12 months from communication, if, pursuant to Article 9(4), the Commission informs the Member State that the draft technical regulation concerns a matter which is the subject of a proposal for relevant EU legislation. Pursuant to Article 9(5), if the Commission adopts a common position during either of the extended standstill periods, then the duty to postpone implementation of the national measure is extended to 18 months.
69. The Commission on 23 April 2010 issued a proposal for a codified version of Directive 98/34/EC to be promulgated, given the number of changes that had been made to its text.²¹ The codification will not affect its substantive content.

(b) Application of the law to the facts

70. BT and TTG provide Information Society services within the meaning of Article 1(2) of the Technical Standards Directive. See Joined Cases C-236-08 to C-238/08 Google France SARL v. Louis Vuitton Malletier SA [2010] ECR I-0000, ECJ at [14], [15] and [110].
71. The contested provisions of the DEA 2010 regulate the provision of Information Society services and constitutes a rule or series of rules on services within the meaning of Article 1(5) of the Directive. The definition of “rule on services” should be given its natural meaning: see Case C-42/07 Liga Portuguesa de Futebol Profissional v. Departamento de Jogos [2009] ECR I-0000, [2010] 1 CMLR 1, ECJ per Advocate General Bot at [164].

which is less restrictive of trade. This system also gives the Commission the necessary time to propose, if necessary, a binding standardisation measure.”

²¹ COM (2010) 179 final.

(i) The Initial Obligations

72. The DEA 2010 through its amendments to the CA 2003 impose two very specific “initial obligations” on ISPs. The nature and extent of these obligations has been repeatedly identified by the Government in the course of the progress of the Digital Economy Bill referred to above.

73. Section 124A CA 2003 requires ISPs to receive and process copyright infringement reports (‘CIRs’) prepared by copyright owners. The ISP must then, pursuant to section 124A(4) notify the subscriber of the CIR. The prescribed contents of that notification are set out in section 124A(6). The notification must include a description of the apparent infringement and the evidence that supports the allegation, including the identification of the subscriber’s IP address and the date and time of the infringement. The notification must also advise the subscriber of how to obtain lawful access to the copyright material and how to prevent unauthorised use. Section 124A(8) sets out a series of further pieces of information or advice that are likely to have to be included in any notification which the ISPs will be required to send out.

74. Section 124B CA 2003 imposes an obligation on ISPs to provide a copyright owner with a copyright infringement list (‘CIL’) if: (a) the owner requests it; and (b) the initial obligations code requires the ISP to provide it. The CIL sets out the number of CIRs which relate to any given subscriber, with the identity of the subscriber replaced with a unique identifier. This will enable the copyright owner to match up any particular infringements with one individual subscriber, provided that a threshold level of infringement has been passed.²²

75. In addition, section 124E CA 2003 sets a significant, prescribed content to be included in the Initial Obligations Code. See sections 124C(6) and 124D(6). The core elements of the prescribed content are:

- 75.1. It must make the required provision for CIRs;
- 75.2. It must make the required provision for notification of subscribers;
- 75.3. It must set a threshold for determining who is a relevant subscriber within the meaning of section 124B(3) CA 2003;

²² The draft Initial Obligations Code issued in May 2010 sets the threshold level for the issue of a CIL at three notifications in respect of any 12 month period. See Exhibit SM-23 at [2.7].

- 75.4. It must state how ISPs are to keep information about subscribers;
- 75.5. It must set limits for the length of time over which ISPs must keep that information;
- 75.6. It must make provision for any costs' contribution devised by section 124M CA 2003;
- 75.7. It must make provision for Ofcom administering, supervising and/or enforcing the Code. The enforcement options will include the ability of Ofcom to set a penalty for each instance of non-compliance of up to £250,000;
- 75.8. It must make provision for subscriber appeals. The requirements for subscriber appeals are themselves fleshed out in section 124K CA 2003. This provision includes a reversal of the usual burden of proof in relation to infringements, pursuant to section 124K(3) and section 124K(6).²³

76. The Code must be either approved or made by Ofcom within six months of the date of entry into force of sections 124A and 124B CA 2003, subject only to a discretionary extension of time which may be granted by the Secretary of State under section 124D(2). Those provisions enter into force on 8 June 2010.

(ii) Technical Obligations

77. Furthermore, section 124G, read together with section 124H and 124J allows the Secretary of State to impose further technical obligations on ISPs to operate in conjunction with a technical obligations code, the content of which is, to a significant extent, prescribed by section 124J. The technical obligations if introduced will form part of a consolidated but two-tier approach to online copyright infringement. The technical obligations build upon the initial obligations and depend for their substantive content on the regime and procedure established by the initial obligations and the relevant definitions.

78. Section 124G(2) defines a technical obligation as an obligation imposed on an ISP to take a technical measure “against some or all relevant subscribers to its service for the purpose of preventing or reducing infringement of copyright by means of the internet.” Technical measures are identified in section 124G(3) as a measure that:

²³ It is not clear that the “defences” available under section 124K(6) CA 2003 will necessarily address the specific grounds included in section 124K(3). The draughtsman’s intention must have been to indicate that the “defences” under section 124K(6) would be available if an admissible ground of appeal is raised.

- 78.1. Limits the speed or other capacity of the service provided to a subscriber;
- 78.2. Prevents a subscriber from using the service to gain access to particular material, or limits such use;
- 78.3. Suspends the service provided to a subscriber; or
- 78.4. Limits the service provided to a subscriber in another way.

79. Section 124J sets out prescribed substantive content for the technical obligations code, to include provisions for enforcement and supervision by Ofcom, the imposition of penalties of up to £250,000 for each instance of non-compliance by an ISP and for subscriber appeals.

(iii) Enforcement provisions

80. Under section 124G(6), ISPs must give Ofcom any assistance it reasonably requires for the purpose of complying with any direction made under section 124G.

81. Furthermore, by virtue of the initial obligations and technical obligations now being incorporated in Chapter 1 of the CA 2003, ISPs regulated by Ofcom may be subject to a direction from Ofcom that they should ensure compliance with the obligations imposed. Such a direction could be given by Ofcom pursuant to sections 45 and 49 CA 2003 as a result of the entry into force of the material provisions on 8 June 2010. Penalties may be imposed for non-compliance with any condition or direction imposed by Ofcom under section 96 CA 2003. Penalties of up to £250,000 may be levied, pursuant to section 124L(2) CA 2003.

82. In addition, pursuant to section 17 DEA 2010, the Secretary of State may make regulations governing the grant of injunctive relief by a Court against an ISP to prevent its service being used to give access to a particular internet location. This is referred to as a blocking injunction. The Court must be satisfied that the location has been, is being or is likely to be used for or in connection with an activity that infringes copyright. Sections 17(4) and 17(5) set out the substantive content that the Regulations must contain:

“(4) The regulations must provide that a court may not grant an injunction unless satisfied that the location is—

- (a) a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright,
- (b) a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or
- (c) a location which has been, is being or is likely to be used to facilitate access to a location within paragraph (a) or (b).

(5) The regulations must provide that, in determining whether to grant an injunction, the court must take account of—

- (a) any evidence presented of steps taken by the service provider, or by an operator of the location, to prevent infringement of copyright in the qualifying material,
- (b) any evidence presented of steps taken by the copyright owner, or by a licensee of copyright in the qualifying material, to facilitate lawful access to the qualifying material,
- (c) any representations made by a Minister of the Crown,
- (d) whether the injunction would be likely to have a disproportionate effect on any person's legitimate interests, and
- (e) the importance of freedom of expression.”

(iv) The requirement for notification of rules on services

83. In Case C-42/07 Liga Portuguesa de Futebol Profissional, (*supra*) the Advocate General at [168] to [172] explained the rationale for the application of the Technical Standards Directive in the context of the provision of Information Society services:

“168. It is clear from the preamble to Directive 98/48 that the Community legislature aimed to extend to specific services of that kind the system of transparency and supervision originally provided for in relation only to goods, so as to avoid the barriers to the free movement of such services which could be caused by national regulations.

169. The application of the mandatory notification system provided for by Directive 98/34 to such regulations does not mean that they are contrary to Community law.

170. As we have seen, Directive 98/34 aims only to establish a system of preventive control. First, by requiring Member States to notify the Commission of any draft technical regulation, the Community legislature asks them to carry out a prior detailed check of its conformity with Community law. Consequently the directive has the effect of making it clear that, if the proposed regulation impedes the free movement of goods or the freedom to provide Information Society services, the Member State must be able to justify it in conformity with the conditions laid down by the case-law.

171. The notification system provided for by Directive 98/34 then enables the Commission and the other Member States to examine the draft regulation to see whether it creates barriers. If so, the other Member States may propose that the author of the draft should amend it. The Commission for its part may propose or adopt joint measures regulating the topic which is the subject of the proposed measure.

172. Such a system reconciles the sovereign power of the Member States to adopt technical regulations in fields where they have not been harmonised with the obligation

they have undertaken to each other in the Treaty to establish a common market, that is to say, a space within which goods and services in particular circulate freely.”

84. The rationale for notification to the Commission of the contested provisions of the Digital Economy Bill (and now the DEA 2010) as “rules on services” is engaged in this case. The imposition of the initial obligations and the prescribed content of the Initial Obligations Code already set out in the DEA 2010 represent restrictions on the free provision of internet access in the United Kingdom. An ISP based in another Member State would be obliged to consider and budget for compliance with the contested provisions of the DEA 2010 if it were considering starting to provide internet access services in the United Kingdom. The Government has recognised that the statutory instrument governing costs-sharing needs to be introduced as soon as possible because ISPs and Ofcom are already incurring costs in implementing the obligations contained in the DEA 2010. See Exhibit SM-20 at [2.3]. The Government has acknowledged that it will have to notify the draft Statutory Instrument governing “costs sharing” to the Commission as a draft technical regulation under the Technical Standards Directive.
85. Furthermore, the technical obligations and the enforcement provisions found in section 17 DEA 2010 will also, if introduced, regulate the activities of ISPs. Those provisions contain substantive content which now cannot be modified except by express statutory amendment by Act of Parliament. If the Secretary of State decides to introduce them the content of these measures will already be fixed, to a substantial extent, by the contested provisions. They constitute rules on services provided by information society service providers and therefore a technical regulation within the meaning of the Technical Standards Directive.
86. The contested provisions of the Digital Economy Bill which gave rise to these obligations were accordingly a draft technical regulation, within the meaning of Directive 98/34/EC as amended. The Act contains particular provisions concerning the service provider, the services and the recipient of services. They constitute either individually or taken as a whole a rule on services. It was only prior to enactment of the Bill that the text of the above obligations could be amended, so as to qualify as a *draft* rule on services. Once enacted, the obligations are incapable of significant amendment through dialogue with interested parties.

87. The United Kingdom was under an obligation to notify the terms of the Digital Economy Bill to the Commission pursuant to Article 8(1) of the Technical Standards Directive. The obligation arose immediately after the Bill was published and introduced to the House of Lords. See Case C-65/05 Commission v. Greece [2006] ECR I-10341, ECJ at [60] and [61]. The reason why such an obligation arose was to enable the Commission, other Member States and other commercial operators to have as much information as possible on the draft technical regulation with respect to its content, scope and general context in order to enable the Commission to exercise as effectively as possible the powers conferred on it by the Directive. See Case C-20/05 Schwibbert [2007] ECR I-9447, ECJ at [41].

(v) *The Defendant's position*

88. In its response to the Pre-action Protocol letter sent by BT to the Secretary of State,²⁴ the Defendant has contended that the provisions of section 124A and 124B which enter into force on 10 June 2010 are mere enabling provisions. He advances the same submission in relation to the technical obligations addressed under sections 124G, 124H and 124J CA 2003 and the blocking injunction provisions in section 17 DEA 2010. He contends that mere enabling provisions need not be notified to the Commission, following the judgment of the ECJ in Case C-194/94 CIA Security International [1996] ECR I-2201, ECJ.

89. There are a number of reasons why this contention is not well founded.

90. **First**, the judgment of the ECJ in Case C-194/94 CIA Security International was premised on the definition of “technical regulation” found in the predecessor Directive 83/189. The Court held at [25] that the contents of part of the national law in issue were not “technical regulations” within the meaning of that Directive, since technical regulations as defined in that measure “are specifications defining the characteristics of products”, whereas the national legislation in issue related to the licensing regime applicable to the provision of security services.

91. That restrictive definition of “technical regulation” no longer applies to the amended definition of technical regulation, which incorporates a rule on services: Case C-42/07 Liga Portuguesa de Futebol Profissional (*supra*) per Advocate General Bot at [164].

²⁴ The Secretary of State with TTG's approval has adopted the same arguments vis-à-vis TTG.

92. The amended definition of “draft technical regulation” provided in the amended Directive 98/34/EC includes a rule on services, including administrative provisions, “formulated with the aim of enacting it or of **ultimately** having it enacted as a technical regulation, **the text being at a stage of preparation at which substantial amendments can still be made.**” In short, the contested provisions of the Digital Economy Bill were a “draft technical regulation” which should have been notified prior to its enactment. It was foreseen that the relevant initial obligations would “ultimately” be enacted. Furthermore, if and when the technical obligations or section 17 Regulations are brought into force, their substantive content has already been determined to a material extent. It was only at the Bill stage that any or any substantial amendments could be made to the basic obligations imposed by the Bill. Enactment of the Bill as the DEA 2010 now precludes any substantial amendment to the content of the obligations as drafted.
93. In other words, the enactment of the Bill as the DEA 2010 now means that the obligations found in sections 124A and 124B will, from their date of entry into force, have legal effect. The fact that certain obligations imposed by sections 124A or 124B will only take effect in practice once an Initial Obligations Code is published does not preclude the obligations being classified as a rule on services. They are prescribed obligations, clear, certain and straightforward in their effect and in the nature of the obligations that are imposed on ISPs. The DEA 2010 clearly envisages that they will ultimately bite on ISPs. Indeed, they are capable of being applied by Ofcom to regulated ISPs with immediate effect through a direction to like effect and could then be the subject of penalties for non-compliance under section 96 CA 2003.
94. Although further detail is to be provided in the Code, this does not mean that the contested provisions are merely enabling provisions. A significant and prescribed set of obligations have been imposed by sections 124A and 124B of the CA 2003. Section 124E prescribes a significant, substantive content for the Code. Ofcom are obliged to bring a default Code into effect within eight months of 8 April 2010, unless the Secretary of State extends the time. At that point, all of the respective obligations will bite. The fact that the practical entry into force of the provisions may not be for some months does not remove the need to notify the measure when it is in draft form. Any more than a delayed entry into force date for a statutory instrument imposing technical standards would obviate the need for notification.

95. The same holds true in respect of the technical obligations imposed by section 124G, 124H and 124J of the CA 2003. These technical obligations are inextricably bound up with the terms of sections 124A and 124B of the CA 2003. The technical measures operate on the premise that, at the stage of their potential deployment, the initial obligations have been complied with and a CIL has been obtained in respect of one or more subscribers. The initial obligations and the technical obligations form part of a coordinated approach deployed by the Act, albeit an approach that has two separate tiers of application.
96. 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. The broad substantive content of the technical obligations has been set. They have a fixed minimum content. Those obligations are also inextricably bound up with the initial obligations. 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. These provisions build upon the foundation of the initial obligations, so that it is important to consider the set of obligations imposed by the DEA 2010 as a composite whole.
97. Finally, while section 17 on its face has more of the appearance of a “pure” enabling provision, in reality it contains a mixture of enabling provisions and substantive requirements, some of which impose concrete obligations and which cannot now be altered by amendment if the Secretary of State exercises his power to introduce Regulations under this section of the Act. Those substantive provisions will govern the provision of services by information society service providers. They are accordingly a draft technical regulation which should have been notified to the Commission.

98. The reasoning of the ECJ in the CIA Security case cannot affect the application of the clear wording of the amended Technical Standards Directive.

99. **Secondly**, even if the reasoning of the Court could be read directly across (*quod non*), it is important to consider the nature and extent of the Court's conclusions in that case. The ECJ in CIA Security held as follows:

“29. A rule is classified as a technical regulation for the purposes of Directive 83/189 if it has legal effects of its own. If, under domestic law, the rule merely serves as a basis for enabling administrative regulations containing rules binding on interested parties to be adopted, so that by itself it has no legal effect for individuals, the rule does not constitute a technical regulation within the meaning of the directive (see the judgment in Case C-317/92 Commission v Germany [1994] ECR I-2039, paragraph 26). It should be recalled here that, according to the first subparagraph of Article 8(1) of Directive 83/189, the Member States must communicate, at the same time as the draft technical regulation, the enabling instrument on the basis of which it was adopted, should knowledge of such text be necessary to assess the implications of the draft technical regulation.

30. However, a rule must be classified as a technical regulation within the meaning of Directive 83/189 if, as the Belgian Government submitted at the hearing, it requires the undertakings concerned to apply for prior approval of their equipment, even if the administrative rules envisaged have not been adopted.”

100. In terms of the Court's ruling on the relevant question referred to it, it concluded that:

100.1. A number of the domestic provisions were indeed technical regulations;

100.2. The requirement for authorisation to conduct business as a security firm was not a technical regulation; and

100.3. The effect of Article 12 of the 1990 Law needed to be viewed in its national context to assess its effect. See [31] of the judgment.

101. The description given of Article 12 of the 1990 law in [6] of the judgment was that certain alarm systems could only be marketed or otherwise made available to users after prior approval had been granted under a procedure to be laid down by Royal Decree. The Court was unable to say for itself whether the effect of that provision in national law gave it legal effect or mere enabled other binding legislation to be introduced in due course.

102. It would therefore follow that an analysis of the effect of the DEA 2010 needs to be undertaken. In this regard, the provisions found in sections 124A, 124B and 124E of the CA 2003 are not “mere” enabling provisions. They contain substantive obligations with

which the Claimants must now comply and which, in practice, are already causing the Claimants to incur significant costs by way of implementation.

103. The content of the initial obligations is detailed and specific. The same point can be made in respect of sections 124G and the broad substantive outline it gives to the technical obligation to impose technical measures if and when introduced. There is no room for the specific content of any of those obligations to be withdrawn, unless the DEA 2010 is repealed. The technical obligations in any event build upon the initial obligations and cannot sensibly be divorced from an overall consideration of the nature and effect of the contested provisions of the DEA 2010. Sections 17(4) and (5) of the DEA 2010 also contain rules governing the substantive content of Regulations which could not be amended at the stage that the Regulations were contained in a draft Statutory Instrument.

104. This point can be seen starkly when considering the Government's own explanation of aspects of the Digital Economy Bill in the Explanatory Notes that accompanied it. Clause 4 (which ultimately became section 124A CA 2003) was described in the following terms in [44] and [47] of the Explanatory Notes.

“44. The section of the 2003 Act that is inserted by this clause (section 124A) **sets out an obligation for ISPs to notify subscribers of copyright infringement reports** (“CIRs”) received about them from copyright owners. It describes what CIRs and notifications to subscribers must contain, the procedures that copyright owners must comply with when making CIRs, and the procedures that ISPs must follow when sending subscriber notifications.

...

47. The notification from the ISP **must** inform the subscriber that the account appears to have been used to infringe copyright, and it **must** provide evidence of the apparent infringement, direct the consumer towards legal sources of content, and provide other advice. The code may require the notification to include other material as well, such as a statement that information about the apparent infringement may be kept and disclosed to the copyright owner in certain circumstances. Further apparent infringements using the subscriber's account may result in additional notifications.” [Emphasis added]

105. Clause 5 (which ultimately became section 125A CA 2003) was described as follows at [48] of the Explanatory Notes:

“48. ISPs **will have to** keep a record of the number of CIRs linked to each subscriber along with a record of which copyright owner sent the report. Under section 124B of the 2003 Act, inserted by clause 5, an ISP may be required to provide a copyright owner with relevant parts of those records on request (“copyright infringement lists”), but in an anonymised form so as to ensure compliance with data protection legislation. The

intention is for the code to set out a threshold number of CIRs, for example 50, which means that a subscriber will be considered a serious repeat infringer whose alleged infringements must be covered by any copyright infringement lists that the ISP provides to the relevant copyright owner.”

106. The Explanatory Notes at [66] stated that “in case the initial obligations prove not as effective as expected, new section 124H gives the Secretary of State the power to introduce further obligations, should that prove appropriate.” The Secretary of State carried out an assessment of the compatibility of the technical obligations with Article 10 of the European Convention on Human Rights. That would have been impossible if the technical obligations were merely enabling provisions. See [236] of the Explanatory Notes to the Digital Economy Bill.²⁵

107. Similarly, section 124E CA 2003 sets down significant, prescribed requirements for the Initial Obligations Code which Ofcom is obliged to approve or adopt of its own volition within a period of eight months from 8 April 2010, subject only to a discretionary extension of time grant by the Secretary of State. In response to concerns voiced in the House of Lords about the legal certainty and lack of detail contained on the face of the Digital Economy Bill, amendments were made to clause 8 to incorporate more elements as mandatory requirements.

108. The Outline Initial Obligations Code issued in January 2010 (Exhibit SM-19) identified these mandatory contents of the Code as follows:

- “Means of obtaining evidence of infringement and standard of evidence to be included in a CIR
- Form of CIR
- Time limit for making a CIR
- Provisions about notification of subscribers – means by which ISP identifies subscribers – which reports ISPs must notify subscribers of
- Requirements about the form, contents and means of notification of subscribers
- How ISPs hold subscriber information and for how long
- Provision about contributions towards costs that are required to be included
- That Ofcom or another have function of administering and enforcing the code, including dispute resolutions (a n other must be sufficiently independent of ISPs and copyright owners (COs) [*sic*]
- A person has function of determining subscriber appeals independent of COs, ISPs and Ofcom.

²⁵ Set out at [79] and [80] of the witness statement of Simon Milner dated 5 July 2010.

- Arrangements for costs related to functions of administering, enforcing the code or determining subscriber appeals must be met by ISPs and Cos
- Code provisions must be objectively justifiable, proportionate, non-discriminatory and transparent.”

109. An updated version of the draft Initial Obligations Code was issued by Ofcom in May 2010 (Exhibit SM-23). It is noteworthy that:

109.1. At [1.3], Ofcom acknowledges that the DEA 2010 is “very clear on how Ofcom should implement many elements of the measures.”

109.2. At [1.6], Ofcom recognises that “as regards those ISPs to whom the Code should apply, the guidance from Government on how we should implement the measures is very clear.” Ofcom has tacitly acknowledged the substantive content of the obligations imposed on ISPs by the Act itself;

109.3. The framers of the Act failed to consider that the establishment of a threshold for application of the Code under section 124C(5) depended on the Code itself being in force so as to give rise to a specific number of CIRs within a particular period. The threshold provisions as presently drafted are therefore unworkable as they give rise to a “chicken and egg” problem. This is recognised by Ofcom at [3.8];

110. **Thirdly**, even if there were any ambiguity as to whether or not the terms of the Digital Economy Bill (and now the DEA 2010) should have been notified to the Commission (*quod non*), that ambiguity should have been resolved in favour of notification. This is so in light of the objectives of the Technical Standards Directive and the obligation imposed on the UK to co-operate sincerely with the Commission in the discharge of obligations imposed by Community law.²⁶

111. The notification and standstill provisions found in the Technical Standards Directive afford the Commission and other Member States the opportunity to examine whether national measures create obstacles to trade, contrary to the TFEU, or obstacles which are to be avoided through the adoption of common or harmonised measures by the EU as a whole. The procedure enables the Commission to propose or adopt EU measures

²⁶ Post the Lisbon Treaty, that obligation is now found in Article 4(3) TEU (formerly Article 10 EC and, before that, Article 5 of the EC Treaty).

regulating the matters dealt with by the envisaged measure. See Case C-194/94 CIA Security (*supra*) at [41].

112. It is settled case-law that Directive 98/34/EC is designed to protect, by means of preventive monitoring, the free movement of goods and services, which are two of the foundations of the EU. The Commission's control serves a useful purpose in that technical regulations falling within the scope of that Directive may constitute obstacles to trade in goods or services between Member States, such obstacles being permissible only if they are necessary to satisfy compelling requirements relating to the public interest. See Case C-303/04 Lidl Italia [2005] ECR I-7865 at [22].

(vi) *The EU perspective*

113. Furthermore, this is an area which is paradigmatically suitable for a co-ordinated approach from the EU. Many of the ISPs operating in the UK are wholly or partly owned by ISPs established in other Member States. The question of unlawful file-sharing is an EU wide problem. Enforcement measures in response need to take into account the possibility of measures of circumvention being adopted if a collective and coordinated response between neighbouring Member States is not adopted. It is eminently foreseeable that, for example, the Commission and Member States may wish to contribute to the debate concerning which measures to tackle unlawful file sharing (both technical and non-technical) might proportionately be imposed.

114. Indeed, as the witness statement of Simon Milner at [135] to [138] makes clear, in October 2009, the European Commission commenced a consultation exercise of its own aimed at the consequences of "de-materialisation of online content." The Reflection Paper issued by the Commission at the same time (Exhibit SM-26) indicated that "the nature of the challenges and problems presented by cross-border provision of creative content by the internet meant that "responses to most of these challenges will have to be joint European ones, instead of being the result of separate or even contradictory national initiatives."

115. There is a possibility that legislative action could be taken at a pan-European level in this area. In November 2009, DG Internal Market and Services published the results of a Study on Online Copyright Enforcement and Data Protection in Selected Member States,

prepared by Hunton & Williams, Brussels.²⁷ The study indicated a number of discrepancies between the approaches in different Member States to online copyright enforcement. It also noted that Member States had given little thought to the interaction between data protection rules and implementation of the IP Enforcement Directive. An updated study setting out the provisions applicable in a further three Member States, including the United Kingdom, was published in May 2010.²⁸

116. The European Digital Agenda adopted by the Commission has envisaged targeted legislative action in this area. The unilateral actions of the UK Government in enacting the DEA 2010 may foreclose the measures that might have been taken at an appropriate EU level.

(vii) Conclusion on Ground 1

117. The effect of the failure to notify is that the provisions of the DEA 2010 are unenforceable. In Case C-194/94 CIA Security International (*supra*) at [44] and [45], the Court described the consequences of failure to notify the Commission. The Court took the view that the obligations of notification and postponement laid down in Articles 8 and 9 of the predecessor Directive 83/189 were unconditional and sufficiently precise to be relied on by individuals before national courts. A technical regulation which has not been notified is therefore unenforceable and national courts must decline to apply it.

118. That case-law can be applied to Articles 8 and 9 of Directive 98/34/EC as they are in similar terms to those of Directive 83/189. See Case C-42/07 Liga Portuguesa de Futebol Profissional (*supra*) per Advocate General Bot at [182]; Case C-303/04 Lidl Italia [2005] ECR I-7865 at [22] and [23]; R (oao Actis SA) v. Secretary of State for Communities and Local Government [2007] EWHC 2417 (Admin) per Charles J at [83] and [84].

(viii) Relief

119. The Claimants contend that the failure to notify the contested provisions of the DEA 2010 renders them unenforceable. They seek declaratory relief to this effect.

²⁷ A copy can be found at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf and at Exhibit SM-27 to the witness statement of Simon Milner dated 5 July 2010.

²⁸ See Exhibit SM-28 to the witness statement of Simon Milner dated 5 July 2010.

(2) Ground 2: infringement of the Electronic Commerce Directive

120. The contested provisions of the DEA 2010 also infringe provisions of 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 ('the E-Commerce Directive').²⁹

(a) The relevant legal provisions

121. Article 1(1) and recital (3) to the E Commerce Directive recognise that the purpose of the Directive is to ensure a high level of legal integration in order to establish a real area without internal borders for information society services. The Directive is aimed at ensuring the free movement of information society services between Member States. In addition, recital (9) states:

“(9) The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.”

122. Recital (10) notes that, in accordance with the principle of proportionality, the measures provided for in the Directive were “strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market.” Article 1(2) accordingly provides that national provisions on information society services are approximated by the Directive only “to the extent necessary” for achieving the objective set out above.

123. Article 2(a) defines information society services formally by reference to Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. Recital (18) notes in terms that “information society services also include services consisting of the transmission of

²⁹ OJ [2000] L No. 178, 17.7.2000, p. 1.

information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service.” In Article 2(d) and recital (20), the definition of recipient of service is broad. It covers “any natural or legal person who, for professional ends or otherwise, uses an information society service.”

124. Article 2(h) defines the “co-ordinated field” covered by the Directive as being “requirements laid down in Member States’ legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.” Article 2(h)(i) makes clear that this includes national measures governing the pursuit of the activity of information society service, “such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider.”

125. Article 3(2) provides that “Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.” Nonetheless, Article 3(4) prescribes the nature of any permissible derogation from this prohibition:

“4. Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:

(a) the measures shall be:

(i) necessary for one of the following reasons:

- public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,
- the protection of public health,
- public security, including the safeguarding of national security and defence,
- the protection of consumers, including investors;

(ii) taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives;

(iii) proportionate to those objectives;

(b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:

- asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate,

- notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures.”

126. Recital (24) to the Directive indicates that it is legitimate for Member States to take measures to restrict the free movement of information society services, but only “under the conditions established in this Directive.” Recital (25) states:

“(25) National courts, including civil courts, dealing with private law disputes can take measures to derogate from the freedom to provide information society services in conformity with conditions established in this Directive.”

127. Article 12, headed “mere conduit”, limits the liability of information society service providers who act as a “mere conduit” in the transmission of information or material. It reads as follows:

“12. 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- (a) does not initiate the transmission;
- (b) does not select the receiver of the transmission; and
- (c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement.”

128. Article 13 contains similar provisions in respect of “caching” of information.

129. At recitals (42) and (43), the Directive explains the basis upon which an exemption from liability is conferred on information society service providers:

“(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of

making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

(43) A service provider can benefit from the exemptions for ‘mere conduit’ and for ‘caching’ when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.”

130. Nonetheless, recitals (44) and (45) also indicate that the exemption will not cover the following types of national action:

“(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of ‘mere conduit’ or ‘caching’ and as a result cannot benefit from the liability exemptions established for these activities.

(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.”

131. A more limited exemption from liability is conferred on “hosting” service providers.

Article 14, headed “Hosting”, states:

“14. 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.”

132. ISPs may provide both “hosting” and access services, but not necessarily to the same customers. Some customers make take storage (or hosting) products separate from access services and vice versa. For those ISPs who do offer “hosting” services, in their role as hosts they have a greater degree of control over the information or material stored by them in respect of those customers taking hosting services. They are accordingly more likely to be able to prevent the commission of an unlawful act than a service provider when providing only access services to a customer and therefore acting as a “mere conduit” in this respect. This means that the same degree of control cannot be exercised (even in respect of the same customers) when access services are provided. Recitals (46) and (47) also explain the extent to which the “host” information society service provider can be tasked with assisting in the prevention of unlawful activities by third parties:

“(46) In order to benefit from a limitation of liability, the provider of an information society service, **consisting of the storage of information**, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.” [Emphasis added]

133. Recital (48) gives a further explanation of the provision for “host” services. It states:

“(48) This Directive does not affect the possibility for Member States of requiring service providers, **who host information provided by recipients of their service**, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.” [Emphasis added]

134. Article 15(1) of the E Commerce Directive provides that Member States shall not impose a general obligation on service providers to monitor the information which they transmit or store, “nor a general obligation actively to seek facts or circumstances indicating illegal activity.” Article 15(2) states:

“2. Member States may establish obligations for information society service providers promptly to 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.”

135. Recital (47) states that:

“(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.”

(b) Application of the law to the facts

136. BT and TTG each provide an information society service. They do so as mere conduit ISPs. As a mere conduit ISP each gives access to an electronic communications network to its own subscribers.. In that capacity, it has neither knowledge of nor control over the information which is transmitted by subscribers. Its actions are merely “technical, automatic and passive.” See Joined Cases C-236-08 to C-238/08 Google France SARL v. Louis Vuitton Malletier SA [2010] ECR I-0000, ECJ, at [110], [113] and [114].

(i) Liability for information transmitted

137. Article 12 of the E Commerce Directive limits the liability that may properly be imposed on BT or TTG as an ISP when they provide mere conduit access services. The combination of the initial obligations, the technical obligations, the costs-sharing provisions (in section 124M CA 2003) and the penalty provisions (found in section 124L CA 2003) in substance and reality impose a liability on the Claimants for the information transmitted by their subscribers or third parties using the subscribers’ internet access over whom they had no control or knowledge. ISPs may have a penalty of up to £250,000 imposed for non-compliance with the contested provisions and are also made to bear the costs of compliance with inadequate compensation for the costs of doing so from the copyright owners. These provisions accordingly infringe Article 12(1) of the E Commerce Directive. The Claimants are each a “mere conduit” for the information transmitted which facilitates unlawful use of file-sharing software by subscribers (or third parties) using their internet access service. The Claimants should not be held accountable for it or be put to any pecuniary detriment as a result of it.

138. The Secretary of State has contended in his pre-action protocol letter of response to BT dated 14 May 2010 that these provisions do not impose liability for information

transmitted by the relevant subscribers. The Secretary of State's focus appears to be a narrow one, assuming that Article 12 precludes vicarious liability for the infringement of copyright by the subscriber. But Article 12 should not be read so narrowly. Whether a measure imposes liability for information transmitted is a question of substance not form. The contested provisions impose substantial financial liability on mere conduit ISPs. Exposure to financial penalties of up to £250,000 a time amounts to such a liability. Furthermore, the cost of compliance with the contested provisions clearly renders the ISPs liable for the information transmitted by the subscribers in that a pecuniary disadvantage is imposed on them as a result of the information transmitted.

139. The contested provisions of the DEA 2010 (with the exception of section 17) are also inconsistent with Articles 13 and 14 of the E Commerce Directive. Those Articles permit an exemption from liability for ISPs providing "caching" or "hosting" services, save where the ISP fails to act expeditiously after having been notified of unlawful activity being perpetrated through the use of its services. Under the DEA 2010, the liability of the ISP after such notification has been extended beyond "caching" and "hosting" services to include the provision of mere "access services." This is contrary to the wording and spirit of the E Commerce Directive.

(ii) Monitoring obligation

140. The requirement imposed by section 124B CA 2003 to maintain lists of infringers based on their internet usage also infringes Article 15. The section in substance and reality requires BT and TTG to monitor the information transmitted to or from subscribers. The information received from copyright owners will inform the ISPs of what the customer has received or sent in the course of an electronic communication. ISPs must then retain that information and monitor all other CIRs notified in respect of the same subscriber. ISPs will end up holding and processing detailed information regarding subscribers' internet usage over the course of time. Technical measures may also give rise to a *de facto* form of real time monitoring, based on internet usage over a period of time. Such a monitoring obligation may only be imposed on a hosting service, pursuant to Article 15(2) of the Directive. It is only hosting services which are capable of exercising the requisite degree of control over the material transmitted to engage in a potential liability (and even then, only in circumstances where they fail to take appropriate care).

141. The European Data Protection Supervisor ('EDPS') has expressed serious concern about similar legislative responses being considered either internationally or in other Member States. At [17] of his Opinion (Exhibit SM-29), he said:

“17. Such practices are highly invasive in the individuals’ private sphere. **They entail the generalised monitoring of Internet users’ activities, including perfectly lawful ones.** They affect millions of law-abiding Internet users, including many children and adolescents. They are carried out by private parties, not by law enforcement authorities. Moreover, nowadays, Internet plays a central role in almost all aspects of modern life, thus, the effects of disconnecting Internet access may be enormous, cutting individuals off from work, culture, eGovernment applications, etc.” [Emphasis added]

142. Further or alternatively, the requirement to compile and maintain lists of CIRs in respect of identified subscribers, coupled with the obligation to provide CILs to copyright owners, also constitute an obligation “actively to seek facts or circumstances indicating illegal activity”, contrary to Article 15(1) of the E Commerce Directive. The ISPs will be required to identify and match an individual subscriber to one or more CIRs. The ISPs must maintain a record of the CIRs received for each such subscriber. They will be required to record and maintain the history of the subscriber’s allegedly infringing behaviour. That history may then be conveyed to the copyright owners through the provision of a CIL, albeit with the subscribers’ identities removed and replaced with a unique identifier.. ISPs will accordingly be obliged to seek the facts and circumstances indicating unlawful activity and pass them on to the copyright owners through CILs.

143. While BT and TTG do provide hosting services, the contested provisions of the DEA 2010 are not confined to hosting services. Unlawful file sharing takes place through access services, not hosting services. Furthermore, the DEA 2010 and the amendments to the CA 2003 impose a general obligation to monitor, rather than an obligation to monitor internet usage in the context of a specific case.

144. The Secretary of State has said in his pre-action protocol letter of response dated 14 May 2010 that the contested obligations do not impose any obligation to monitor or store information and no obligation is imposed actively to seek facts or circumstances indicating illegal activity. The suggestion to the contrary is without foundation. The Claimants disagree and note that the EDPS Opinion, provided by the individual responsible for supervision of data protection at the EU level, supports their view.

(iii) Removal or disabling of access to information

145. The technical obligations imposed by sections 124G, 124H and/or 124J and the Regulations prescribed by section 17 DEA 2010 also impose or permit measures which govern “the removal or disabling of access to information.” Such measures may only be taken against a “hosting” or storage service, and not against an ISP which acts as a mere conduit. This follows from the obvious contrast between Article 12(3) of the Directive (which applies to mere conduits) and Article 14(3) which applies to hosts. Again, unlawful file sharing is not connected to any hosting services that BT or TTG may incidentally offer to its subscribers. The obligations imposed and/or envisaged by the DEA 2010 bite in respect of the provision of access services by the Claimants.

146. Article 12(3), set out at paragraph 127 above states that:

“3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement.”

147. Article 14(3) on the other hand, set out at paragraph 131 above, states that:

“3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, **nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.**”

148. The Secretary of State has asserted that this contrast in wording between Article 12(3) and Article 14(3) does not preclude the imposition of the measures in question on mere conduit ISPs. But the possibility for Member States to establish procedures governing the removal or disabling of access to information applies only in relation to hosting services. The technical obligations and section 17 DEA 2010 envisage such measures being taken in respect of access services provided by ISPs as well. Had the EU wished to permit Member States to adopt such measures in respect of access services, its legislation would have said so in terms.

149. The Claimants acknowledge that Article 12(3) does not preclude the possibility for a court or administrative authority, in accordance with Member States’ legal systems,

requiring the service provider to terminate or prevent an infringement. A court or an administrative authority may, if the domestic law of a Member State provides for it, require ISPs to disclose to private third parties personal data relating to internet traffic in order to enable them to bring civil proceedings for copyright infringement, provided that such measures comply with general principles of EU law, including the principle of proportionality (as to which see Ground 4). See, by analogy, Case C-557/07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH [2009] ECR I-1227, ECJ at [41] (which expressly refers to the E Commerce Directive).

150. But the online copyright infringement provisions in the DEA 2010 do not benefit from this derogation from the restrictions on liability of “mere conduits.” The DEA 2010 imposes technical measures without recourse to a direction from a Court or administrative authority. The technical measures apply without any requirement for prior scrutiny by a Court or administrative authority. A subscriber may bring an appeal against any technical measure imposed, but his internet access will be curtailed by an ISP simply on the basis of evidence received from a copyright owner where, for example, he has not appealed within a specified time period. Furthermore, the appeal mechanism provided is deeply flawed, since it essentially transfers the burden on the subscriber to prove a negative, namely that he or she was not the person who participated in the unlawful file-sharing associated with the subscriber’s IP address. This will be excessively difficult in any event, and particularly in circumstances where the subscriber’s IP address has been unlawfully “hacked into” by third parties. The contested provisions require ISPs to become the “enforcer” or policeman in respect of copyright infringements. The technical measures also impose general obligations which are not directly aimed at preventing or terminating any particular infringement. This means that the wheat of innocent usage is caught with the chaff of unlawful file sharing.

151. The Court is respectfully invited to note that issues concerning the correct interpretation of Articles 12 and 14 of the E Commerce Directive have already been subject to three pending references to the European Court of Justice in the following cases:

- 151.1. Case C-323/09 Interflora Inc v. Marks & Spencer plc (reference from the English High Court, Chancery Division);³⁰
- 151.2. Case C-324/09 L'Oréal SA v. eBay International AG (reference from the English High Court, Chancery Division);³¹
- 151.3. Case C-70/10 Scarlet Extended SA v. SABAM (Cour d'Appel, Bruxelles, Belgium).³² In this case, the referred questions are as follows:

“1. Do Directives 2001/29 and 2004/48, in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: ‘They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right’, to order an Internet Service Provider (ISP) to introduce, for all its customers, *in abstracto* and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?

2. If the answer to the question in paragraph 1 is in the affirmative, do those directives require a national court, called upon to give a ruling on an application for an injunction against an intermediary whose services are used by a third party to infringe a copyright, to apply the principle of proportionality when deciding on the effectiveness and dissuasive effect of the measure sought?”

152. The contested provisions of the DEA 2010 are also capable of applying to an ISP established in another Member State. This has been recognised by the fact sheets provided by DBIS: see Exhibit SM-15. The DEA 2010 imposes restrictions on the free provision of internet services by ISPs, including those established in other Member States.

153. The United Kingdom is entitled to adopt measures derogating from the free provision of services, but only if the conditions set out in Article 3(4) of the E Commerce Directive

³⁰ OJ [2009] C No. 282, 21.11.2009, p. 19.

³¹ OJ [2009] C No. 267, 7.11.2009, p. 40.

³² OJ [2010] C No. 113, 1.5.2010, p. 20.

are satisfied (see paragraph 125 above for Article 3(4)). Those conditions are not satisfied in this case, since:

- 153.1. The Government has failed to establish that the measures in question are strictly necessary for the protection of public policy;
- 153.2. The measures have not been taken on a specific and targeted basis against one or more ISPs who are shown to present a serious and grave risk of prejudicing such public policy objective as might be identified;
- 153.3. The measures are not proportionate, for the reasons set out in Ground 4 below;
- 153.4. In any event, the Secretary of State has not notified the Commission of its intention to take such measures, contrary to Article 3(4)(b) of the E Commerce Directive.

(iv) Relief

154. The Claimants seek a quashing order in respect of all or part of the contested provisions of the DEA 2010 that infringe the E Commerce Directive or a declaration that such provisions are to be dis-applied by virtue of their incompatibility with the above provisions.

(3) Ground 3: infringement of the Directive on privacy and electronic communications

155. Further or alternatively, the contested provisions in the DEA 2010 infringe relevant provisions of 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 ('the PEC Directive').³³

(a) The relevant legal provisions

156. Article 1 of the Directive on privacy and electronic communications states:

“1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the

³³ OJ [2002] L No. 201 p. 37.

right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.”

157. Pursuant to recital (2) to the Directive, the rights enshrined in Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of fundamental rights of the European Union are to be respected in particular. By Article 1(2) and recital (1) to the Directive, the PEC Directive is intended to complement 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 (‘the Data Protection Directive’).³⁴

158. Article 2(b) defines “traffic data” as “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.” Under Article 2(d), communication is defined as follows:

“... any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.”

159. By Article 3(1), the PEC Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. Article 5(1) of the PEC Directive provides that:

“Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.”

160. Article 5 requires Member States to ensure that the confidentiality of communications and related traffic data by means of a public communications network is respected under national legislation. Domestic legislation must prohibit listening, tapping, storage or other

³⁴ OJ [1995] L No. 281, 23.11.1995, p. 31.

kinds of interception or surveillance of communications and related traffic data by persons other than users, without either: (a) the consent of the user; or (b) a legally permissible authorisation to do so under Article 15 of the PEC Directive. This requirement is expressed not to prevent technical storage of data which is necessary for the conveyance of a communication, while protecting its confidentiality. In addition, Article 5(2) permits the legal authorisation of recording of communications and related traffic data carried out for specific purposes in the course of lawful business activity.

161. The material parts of Article 6 provide as follows:

“1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.”

162. The limited circumstances under which a service provider may legitimately process traffic data are explained further in recitals (26) to (32) of the Directive.

163. These restrictions on the retention of data should also be read with in conjunction with the provisions of the European Parliament and EC Council Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (the ‘Data Retention Directive’).³⁵ Article 4 of that Directive requires that Member States adopt measures to ensure that data retained in accordance with the Directive “is provided only to the competent national authorities in specific cases and in accordance with national law.”

³⁵ OJ [2006] L No. 105, 13.04.2006, p 54.

164. Article 15 of the PEC Directive concerns the application of certain provisions of Directive 95/46/EC. It reads:

“1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.”

(b) Application of the law to the facts

165. The contested provisions in the DEA 2010 (and, in particular, the initial obligations found in section 124B CA 2003) require the Claimants to process and make available personal data, within the meaning of Article 2 of the PEC Directive and Article 2(a) and (b) of Directive 95/46/EC. See Case C-275/06 Productores de Música Española (Promusicae) [2008] ECR I-271, ECJ at [45]. The provisions also infringe the subscribers’ right to confidentiality of communications and related traffic data.

(i) Infringement of the PEC Directive

166. Information passed by copyright owners to ISPs concerning the use of the internet by individuals constitutes personal data, particularly in the hands of the ISP. If, as it should, the CIR also identifies the nature of the digital material downloaded or uploaded by an individual then it is perfectly possible that the CIR will contain special categories of personal data within the meaning of Article 8 of the Data Protection Directive, relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or relating to health or sex life of an individual.

167. Both copyright owners and ISPs will process that personal data in the course of sending and receiving CIRs and CILs. In order lawfully to process such data, one of the criteria in Article 7 of the Data Processing Directive must be met. If the data also consists

of a special category of personal data, then data processing is generally prohibited unless one of the exceptions under Article 8(2) of the Data Processing Directive is engaged. To the extent that the enforcement of the obligations found in the DEA 2010 in due course catches sensitive personal data, the UK Government will also be in breach of its obligation to notify derogations under Article 8 to the EU Commission.

168. The information processed by ISPs and further disclosed to copyright owners is also traffic data within the meaning of Article 2 of the PEC Directive. There are additional and fundamental restrictions placed on the processing of traffic data in context of electronic communications. In the light of its potentially intrusive nature, traffic data can (subject to certain exceptions) be processed only for limited purposes set out in Article 6 of the PEC Directive.

169. Article 6(1) of the PEC Directive also contains an express requirement that traffic data should be anonymised or erased when it is no longer needed for the purpose of transmission of a communication (i.e. the primary purpose) or for one of the limited additional purposes permitted, namely:

- 169.1. Subscriber billing/ interconnection payments;
- 169.2. The marketing electronic communications;
- 169.3. The provision of value added services.

170. The processing by ISPs of traffic data required and/or envisaged by the DEA 2010 does not fall into any of those categories. It follows that it can only be justified by way of a derogation from these requirements pursuant to Article 15 of the PEC Directive.

171. Article 15 imposes certain requirements before a derogation will be allowed. These are that the measure should be:

- 171.1. Necessary, appropriate and proportionate;
- 171.2. Required to safeguard national security (i.e. State security), defence, public security, and the prevention detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of the Data Protection Directive;
- 171.3. Limited in duration;

171.4. Consistent with the general principles of EU law, including those referred to in Articles 6(1) and 6(2) TEU (now Articles 6(1) and 6(3) TEU)).

(ii) The Defendant's response

172. In its pre-action protocol letter, the Secretary of State relies upon the judgment of the ECJ in Promusicae (*supra*) and contends that there is no reason to confine the scope of its application to civil proceedings. It is true that in Promusicae at [54], the Court recognised that the PEC Directive did not preclude Member States from laying down an obligation to disclose personal data in the context of civil proceedings.

173. But the Secretary of State is wrong to suggest that the reasoning extends beyond the context of civil proceedings. At [70] the ECJ in Promusicae held that any obligation to disclose personal data had to be in order to ensure “the effective protection of copyright in the context of civil proceedings.” The obligations set in place by the DEA 2010 require disclosure (CIRs and CILs) other than in the context of civil proceedings. There is no judicial oversight in the process at all. Nor is the extent and ambit of the disclosure tailored to the individual circumstances of the case as a result of the exercise of regulatory judgment by an administrative authority. The appellate mechanism set out in section 124K CA 2003 need never be engaged and is, in any event, deeply flawed for the reasons set out above.

174. The contested provisions of the DEA 2010, unlike the common law principles found in the *Norwich Pharmacal* line of cases, do not take place in the “context of civil proceedings.” They require the Claimants to maintain and make available CILs in circumstances where civil proceedings may never be brought. Furthermore, unlike in *Norwich Pharmacal* cases, the Claimants are obliged to bear the costs of processing and making available this private data with only inadequate reimbursement for doing so.

175. In any event, at [64] of the Promusicae judgment, the Court also recognised that any obligation to disclose confidential personal data had to respect Articles 7 and 8 of the Charter of Fundamental Rights, requiring protection to be given to the right to respect for family and private life and the right to the protection of personal data.

176. At [68], the ECJ held that:

“That being so, the Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must 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 (see, to that effect, Lindqvist, paragraph 87, and Case C-305/05 Ordre des barreaux francophones et germanophone and Others [2007] ECR I-0000, paragraph 28).”

177. In order to implement the regime established and/or envisaged by the DEA 2010, copyright owners must themselves compile and process personal data relating to individuals (or data that is in any event personal data in the hands of the ISP). This may include sensitive data in certain circumstances, such as where the choice of downloaded material reveals intimate details about the subscribers’ private life. The DEA 2010 does not expressly authorise copyright owners to process this data. It follows that the regime is premised on an unlawful foundation. The European Data Protection Supervisor has rightly questioned the legal basis for such processing, in [51] to [52] of his opinion dated 22 February 2010 (Exhibit SM-29).

178. Article 6 of the PEC Directive also imposes an obligation on ISPs to anonymise and/or erase traffic data once it is no longer required for a business purpose. There is in fact no express obligation in the DEA 2010 compelling ISPs to retain the relevant information for any period of time when it is no longer required for business purposes. There is no obligation to retain it as such, even if a CIR is filed, let alone an obligation to retain the data as a precautionary measure, lest a CIR be filed. Absent an express requirement to retain this information, no derogation under Article 15 can be relied upon. Any implied obligation that the Secretary of State might seek to impose would fail to comply with the general EU law principle of legal certainty.

179. The obligations imposed and/or envisaged by the DEA 2010 also contain a requirement for additional processing of the data beyond its mere retention and disclosure. In particular, ISPs must:

- 179.1. Ensure that they are able routinely and accurately to match ISP addresses to subscriber details across their entire customer bases. This applies to both dynamic and static IP addresses, despite the technological complexities involved;
 - 179.2. Upon receipt of a CIR, notify the subscriber in question and communicate to him the detailed information of the type set out in section 124A(6) CA 2003;
 - 179.3. Compile and retain (for an unspecified period) databases containing CILs that match CIRs to specific, relevant subscribers;
 - 179.4. Disclose CILs to copyright owners upon the latter's request;
180. There is also a risk that ISPs may be required (under the finalised initial obligations code) to take reasonable steps to ensure that they are able match IP addresses to subscriber information in circumstances where they cannot now. This might cover the permitted use of a public 'wifi' service or the provision of wireless internet access on a "subscriber-less" pay as you go system, or in return for tokens etc. It is also likely that ISPs will have to undertake further processing in order to administer any technical measures that are imposed.
181. It is neither necessary, appropriate nor proportionate for an ISP to be required to undertake this additional processing in circumstances where it is required to bear all or a substantial part of the cost of doing so, and where the processing goes beyond the ambit of its own business activities and interests, in order to protect the rights of unconnected third parties. This is particularly so where private law remedies already exist at common law to protect the copyright owners, but where rights holders have been reluctant to vindicate their own rights by reference to them. See [64] to [66] of the witness statement of Andrew Heaney dated 5 July 2010.
182. It is noteworthy that even in the context of the Data Retention Directive, the obligation to retain data is limited to that data generated or processed in the normal course of business activity. See Article 3 of that Directive. The extended obligation imposed or envisaged by the DEA 2010 to retain data beyond that permitted by Article 3 is unlawful and beyond the scope of the permissible derogation allowed by Article 15 of the PEC Directive.

183. In Case C-275/06 Productores de Música España (Promusicae) (*supra*) Advocate General Kokott at [106] noted that: “It is however not certain that private file sharing, in particular when it takes place without any intention to make a profit, threatens the protection of copyright sufficiently seriously to justify recourse to this exception. To what extent private file sharing causes genuine damage is in fact disputed.”
184. The contested provisions are not a proportionate response to the issue, as required by Article 15 of the Directive on privacy and electronic communications. BT and TTG rely upon the facts and matters set out in Ground 4. They also rely upon the conclusions of the European Data Protection Supervisor in his opinion dated 22 February 2010 (found at pages 14 to 19 of Exhibit SM-29). These conclusions (in relation to similar legislation) were that such measures were unlikely to be proportionate because:
- 184.1. The (unnoticed) monitoring would affect millions of individuals and all users, irrespective of whether they are under suspicion;
- 184.2. The monitoring would entail the systematic recording of data, some of which may cause people to be brought to civil or even criminal courts; furthermore, some of the information collected would therefore qualify as sensitive data under Article 8 of Directive 95/46 which requires stronger safeguards;
- 184.3. The monitoring is likely to trigger many cases of false positives. Copyright infringement is not a straight ‘yes’ or ‘no’ question. Often Courts have to examine a very significant quantity of technical and legal detail over dozens of pages in order to determine whether there is an infringement;
- 184.4. The potential effects of the monitoring, which could result in disconnection of Internet access. This would interfere with individuals’ right to freedom of expression, freedom of information and access to culture, e-Government applications, marketplaces, email, and, in some cases, with work-related activities. In this context it is particularly important to realise that the effects will be felt not only on the alleged infringer, but all the family relatives that use the same Internet connection, including school children who use the Internet for their school activities.
- 184.5. The fact that the entity making the assessment and taking the decision will typically be a private entity (i.e. the copyright holders or the ISP). The EDPS already stated in a previous opinion his concerns regarding the monitoring of individuals by

the private sector (e.g. ISPs or copyright holders), in areas that are in principle under the competence of law enforcement authorities.

(iii) Relief

185. The Claimants seek a quashing order in respect of all or part of the contested provisions of the DEA 2010 that infringe the PEC Directive or a declaration that such provisions are to be dis-applied by virtue of their incompatibility with the above provisions.

(4) Ground 4: proportionality

186. The contested provisions represent a disproportionate restriction on the free movement of services and/or the right to privacy and/or the right to free expression or to impart and receive information.

(a) Relevant legal principles

187. Article 56 TFEU (ex Article 49 EC) coupled with Article 61 TFEU (ex Article 55 EC) and Article 52 TFEU (ex Article 46 EC) prohibit restrictions on the free movement of services and/or the freedom of establishment,³⁶ save where they are justified in the public interest and proportionate. Article 56 TFEU requires the abolition of all restrictions on the freedom to provide services, even if those restrictions apply without distinction to national providers of services and to those from other Member States, when they are liable to prohibit, impede or render less advantageous the activities of a service provider established in another Member State where it lawfully provides similar services. See Case C-42/07 Liga Portuguesa de Futebol Profissional v. Departamento de Jogos [2009] ECR I-0000, ECJ at [51]; and Case C-369/96 and C-376/96 Jean-Claude Arblade v. Bernard Leloup [1999] ECR I-8453, at [33].

³⁶ The distinction between the right of establishment and the freedom to provide services has not always been clearly drawn by the ECJ in its case law. Nonetheless, in Case C-171/02 Commission v. Portugal [2004] ECR I-5645, ECJ at [24] and [25].

188. The requirement for the contested provisions in the DEA 2010 to be proportionate also arises from the terms of Article 3(4) of the E Commerce Directive and Article 15 of the PEC Directive. Article 15 of the PEC Directive also requires the contested provisions to comply with the general principles of EU law, including those referred to in Article 6(1) and what is now 6(3) TEU (following the renumbering of the TEU in the Lisbon Treaty).
189. The application of a host Member State's national rules to a cross-frontier provider of services is liable to prohibit, impede or render less attractive the provision of services to the extent that it involves expenses and additional administrative and economic burdens. See Case C-165/98 Mazzoleni v. Inter Surveillance Assistance SARL [2001] ECR I-2189, at paragraph 24.
190. This rule is for the benefit of service providers and recipients. See Joined Cases 286/82 and 26/83 Luisi and Carbone [1984] ECR 377, ECJ at [16]. So Article 56 TFEU will, in principle, prohibit a restriction on the freedom of the residents of the Member State concerned to enjoy, via the internet, services which are offered in other Member States. See Case C-42/07 Liga Portuguesa de Futebol Profissional (*supra*) at [53].
191. Articles 61 TFEU and 52 TFEU permit restrictions justified on grounds of public policy, public security or public health. In addition, a certain number of overriding reasons in the public interest have been recognised by case law, such as the objectives of consumer protection and the prevention of both fraud and incitement to squander money on gambling, as well as the general need to preserve public order. See Case C-42/07 Liga Portuguesa de Futebol Profissional (*supra*) at [53].
192. While it is for the Member States to decide on the degree of protection which they wish to afford to public policy interests and on the way in which that protection is to be achieved. They may do so, however, only within the limits set by the Treaty and must, in particular, observe the principle of proportionality. See Case C-429/02 Bacardi France v. TF1 [2004] ECR I-6613, ECJ at [32]. The measures adopted must be appropriate to

secure the attainment of the objective which they pursue and not go beyond what is necessary in order to attain it.³⁷ All such derogations are strictly construed.³⁸

193. In relation to the case law on overriding or imperative requirements, the ECJ in Joined Cases C-369/96 and C-376/96 Arblade and Others [1999] ECR I-8453, at [34] and [35] also pointed out the restrictions which apply to any derogation from the fundamental principle of the free movement of services.

“34. Even if there is no harmonisation in the field, the freedom to provide services, as one of the fundamental principles of the Treaty, may be restricted only by rules justified by overriding requirements relating to the public interest and applicable to all persons and undertakings operating in the territory of the State where the service is provided, in so far as that interest is not safeguarded by the rules to which the provider of such a service is subject in the Member State where he is established . . .

35. The application of national rules to providers of services established in other Member States must be appropriate for securing the attainment of the objective which they pursue and must not go beyond what is necessary in order to attain it.”

194. In addition, Article 8 of Directive 2004/48/EC of 28 April 2004 on the enforcement of intellectual property rights (‘the IPRE Directive’)³⁹ states that ISPs may be ordered by competent judicial authorities to provide personal information that they hold about alleged infringers (e.g. information on the origin and distribution networks of the goods or services which infringe an intellectual property right) in response to a justified and proportionate request in cases of infringements on a commercial scale. The EU legislature clearly considered this was an appropriate standard to follow in the context of any proportionality assessment.

195. Furthermore, as is apparent from the various legislative provisions set out above, the DEA 2010 must respect the principles enshrined in the European Convention on Human Rights (‘ECHR’) and the EU Charter of Fundamental Rights relating to the right to privacy and the right to free expression. This obligation arises from:

195.1. Article 6(1) TEU, which states that the Union recognises the rights, principles and freedoms set out in the Charter of Fundamental Rights of the European Union of

³⁷ See Joined Cases C-1/90 and C-176/90 Aragonesa de Publicidad Exterior and Publivia [1991] ECR I-4151, ECJ at [16].

³⁸ See Case 352/85 Bond van Adverteerders [1988] ECR 2085, ECJ at paragraph 36; Case C-348/96 Criminal proceedings against Donatella Calfa [1999] ECR I-11, at paragraph 23.

³⁹ OJ [2004] L No 157, 30.4.2004, p. 45.

7 December 2000 (as adapted at Strasbourg in December 2007) “which shall have the same legal value as the Treaties.”

195.2. Article 6(3) TEU. This states that:

“Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union’s law.”

195.3. General principles of EU law. The principles of the ECHR also infuse the general principles of EU law, and apply to Member States who implement regimes derived from EU law or who act in a field which is subject to EU competence. See Joined Cases C-20/00 and C-64/00 Booker Aquaculture [2003] ECR I-7411 at [46], [64] to [67] and [88];

195.4. The requirements of the Framework Directive, as amended. Changes to the Telecommunications Framework Directive have been made by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/12/EC on a common regulatory framework for electronic communications, networks and services, 2002/19/EC on access to, and interconnection of, electronic communications, networks and associated facilities, and 2002/20/EC on the authorization of electronic communications, networks and services.⁴⁰ The amendments made by Directive 2009/140/EC do not have to be transposed by Member States until 25 May 2011, but the United Kingdom must refrain from taking any measures liable seriously to compromise the result prescribed.⁴¹ Article 1(3a) of the Framework Directive as amended provides that:

“Measures taken by Member States regarding end-users’ access to, or use of, services and application through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the [ECHR] and general principles of Community law.”

195.5. Equivalent rights conferred by Articles 7, 8, 11 and 52 of the Charter of Fundamental Rights of the European Union⁴² and Article 6(1) TEU; and/or

⁴⁰ OJ [2009] L No 337, p. 37.

⁴¹ Case C-129/96 Inter-Environment Wallonie ASBL v. Région Wallonne [1996] ECR I-6775, ECJ, at [40] to [45].

⁴² OJ [2000] C No. 364, p. 1.

195.6. The Human Rights Act 1998.

196. In this regard, Article 8 ECHR provides that:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

197. Article 10 ECHR states:

“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.”

198. Article 8 of the Charter of Fundamental Rights recognises a discrete right to protection of personal data:

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”

(b) Application of law to the facts

199. The contested provisions of the DEA 2010 represent a restriction on the free movement of services and/or an interference with the right to privacy and/or the right freely to receive or impart opinions and information. The burden accordingly falls on the United Kingdom to present a public policy justification for such measures and to establish that the measures are proportionate to the aim to be achieved.

200. While the United Kingdom has not formally stated that it relies upon the need to protect the rights or property of others as a justification for the measure, it seems likely that it will do so.

(i) The DEA 2010 offends the principle of proportionality

201. The Claimants contend that the contested measures as presently formulated are not proportionate to the legitimate aim of protecting the rights of others, for the reasons set out in detail in the experts' report of Professor Robin Mansell of the London School of Economics and Professor Edward Steinmueller of the University of Sussex dated 1 July 2010, the witness statement of Andrew Heaney dated 5 July 2010 at [20] to [68] and the witness statement of Simon Milner dated 5 July 2010 at [139] to [149]. In summary, this is for all or some of the following reasons.

202. **First**, the contested provisions of the DEA risk catching and harming innocent internet users whose internet service has been used for illicit purposes by third parties. The procedure for detecting potential infringers is based on copyright owners identifying an IP address of an individual file-sharing on a P2P site. That IP address is then matched by an ISP to a particular connection and subscriber. It is then that subscriber who receives the notification and who is then included on the CIL, potentially to be provided to copyright owners and further potentially exposed to litigation based on his or her inclusion on the CIL. Further, if the envisaged technical obligations are implemented that innocent subscriber could have his or her internet service disconnected. But as the witness statement of Mr. Heaney makes clear, at [41] to [42], such a process is inherently unreliable in identifying the actual infringer. Users of the internet connection may include not only friends and family of the subscriber, and other legitimate users unknown to the subscriber, but also those who unlawfully "hack into" the subscriber's network. The ease with which such hacking can be done is apparent from Mr. Heaney's statement. Pursuant to section 124K(6) CA 2003, the burden will be on the innocent subscriber wishing to avoid the various sanctions to show that they took certain measures to protect their internet connection and also show that they themselves did not commit the infringement.

203. **Secondly**, the contested measures will have a chilling effect on internet use that goes well beyond the objective of penalising unlawful file-sharers. The initial obligations

coupled with the terms of section 124K(6) CA 2003 impose an obligation on subscribers to take reasonable steps to ensure that their networks are not mis-used. The technical measures if imposed will severely dissuade and/or impede the ability of a number of consumers, businesses, institutions and other organisation to access the internet, even if they have taken all reasonable steps to prevent the use of their IP address for unlawful copyright infringement. These measures will also negatively affect those organisations that provide or use open wifi, such as coffee shops, libraries and universities.

204. For example, the Government's own fact sheet relating to Libraries, Universities and Wi-Fi Providers issued in February 2010 (Exhibit SM-15) recognised that public libraries and universities might find themselves caught by the contested provisions, either as ISPs or subscribers. It also recognised that "hotels, holiday parks and conference centres will in many cases offer a level of service where infringement could become a significant problem." The Secretary of State's suggested solution is for these organisations to take a range of measures including investing in private software that would prevent P2P file-sharing. This, of course, is no solution for universities who depend on P2P file-sharing for complex academic studies.

205. **Thirdly**, the proportionality assessment conducted by the Government was vitiated by errors of law in that it failed properly to take into account material considerations and took into account irrelevant considerations. It also was premised on data provided to the Government by copyright owners or their representative bodies, which has not been objectively verified or subject to independent scrutiny:

205.1. It failed properly to take into account the strong likelihood of unlawful file-sharers taking steps to circumvent the measures and the ease with which they could do this using a multitude of easy alternatives to P2P file-sharing. The implication of this is that the increase in revenue resulting from the measures will be much smaller than the Government estimated;

205.2. The legislative impact assessment conducted by the Government expressly declined to take into account the costs (or disbenefits) to digital product consumers that would result from their reduced consumption, since the content was said only to be available illegally. The Government's justification for this appeared to be that it should be omitted since the activity is illegal. However, such an approach is not economically sound. Furthermore, US evidence (identified in the Impact

Assessment) had apparently indicated that the monetised cost if this were taken into account would be at least double the monetised benefit to rights holders;

205.3. Indeed, a number of studies referred to in the Impact Assessment⁴³ have in fact found that the displacement effect of P2P downloading was zero. In other words, demand for legal content would not increase if unlawful file sharing is prevented. If that is right, the costs of the DEA 2010 would vastly outweigh the benefits, which would be negligible;

205.4. The witness evidence of Mr. Heaney identifies a number of other costs' components which were left out of account, including:

205.4.1. The cost of upgrading home and business networks to comply with the requirement for reasonable steps to be taken under section 124K(6) CA 2003;

205.4.2. The chilling effect on open wifi networks and other computer networks that provide a public benefit, such as libraries and universities;

205.4.3. The distress occasioned to those falsely accused of unlawful activity;

205.4.4. Distress to those whose personal details are disclosed to subscribers;

205.4.5. Customer service costs for ISPs related to the regime generally;

205.4.6. The detrimental impact on ISPs goodwill and harm to their reputation;

205.4.7. Additional migration costs and competitive distortion occasioned by subscribers moving to other ISPs not proposed to be included in the scope of the Initial Obligations Code;

205.4.8. The true costs of the appellate process;

205.4.9. Harm and loss associated with the disconnection of internet accounts under the technical measures;

205.4.10. The costs of data protection compliance.

206. **Fourthly**, the Impact Assessment conducted by the Government was fundamentally flawed (and therefore *Wednesbury* unreasonable) in its analysis of the benefits of the contested provisions. In particular:

206.1. The data relied upon by the Government to establish a net annual benefit to copyright owners of £400 million was not subject to sufficient independent scrutiny. At least one of the reports relied upon has not been made publicly available;

⁴³ The two studies which had reached this conclusion were identified in the Impact Assessment, (Exhibit SM-14), Table 1 at page 107. These were studies that had been based on actual downloads data, rather than surveys or download proxies data.

- 206.2. The analysis assumed that an unrealistically high proportion (50%) of the displaced revenue would be recovered by copyright owners if the provisions deterring and preventing unlawful file sharing were introduced. This ignores the ease with which such measures may be circumvented and over-stated the likely commercial demand for lawful product, for the reasons set out in the experts' report at pages 14 to 16 and the witness statement of Mr. Heaney at [29] to [31];
- 206.3. The Government's analysis uses the wrong economic measure of benefit and wholly fails to take into account consumer welfare or the consumer surplus that may accrue from the availability of digital content over the internet. The Impact Assessment expressly did not take into account the consumer benefit from file sharing, thus invalidating the entire basis of the comparison between benefit to consumers and detriment to the copyright owners;
- 206.4. The Claimants will also rely upon the facts and matters set out above (in particular at paragraph 205) and more generally in the witness evidence of Mr. Heaney dated 5 July 2010 and Mr. Milner dated 5 July 2010.
207. The proportionality assessment made by the Secretary of State is also flawed for the reasons set out in the expert report of Professors Robin Mansell and Professor Edward Steinmueller dated 1 July 2010. In particular:
- 207.1. The revenue loss associated with subscribers leaving the Claimants and other ISPs in favour of those providers who are exempted from the obligations under the draft Initial Obligations Code were not properly taken into account by the Government in its impact assessment. Nor was the impact on the ISPs goodwill taken into account;
- 207.2. The costs for schools, libraries and other public organisations, as well as for business and users in the "third sector", in responding to the measures were not taken into account;
- 207.3. Reputational detriment associated with the occurrence of false positives was not taken into account in the consultation process;
- 207.4. The perception by subscribers that they were being "monitored" would have a negative impact on their beneficial use of the internet. Feelings of mistrust which arise as a result of the intrusion with subscribers' privacy and the imposition of the role of "policeman" on ISPs could give rise to a substantial negative impact on demand for ISPs' services;

- 207.5. There is a risk that infringers will simply find alternative ways of unlawfully sharing digital file content, thus circumventing the elaborate measures the Government has put in place. This will include such users switching to those ISPs who are not proposed to be covered by the DEA 2010 and developing different methods of avoiding detection or exchanging the material;
- 207.6. There may well be a curtailment of the use of the internet in public places, the social cost of which has not been calculated;
- 207.7. There is at best mixed evidence as to the extent to which the prevention of unlawful file sharing would significantly improve revenues for rights holders;
- 207.8. The Government's analysis of the likely additional revenues to be achieved by the rights holders proceeds on a fundamentally flawed basis in that it cannot be assumed that users who are deterred from receiving a product for no price would be willing to pay the full asking price for it. They may simply decline to consume the product. An increase in the price of a product will, following conventional economic theory, reduce the demand for it;
- 207.9. The methodology used for assessing the revenue benefit to rights' holders was highly speculative. The suggestion that the revenue benefit would persist for a decade was highly implausible;
- 207.10. There was therefore a significant skew in favour of the rights' holders position in the Impact Assessment conducted by the Government in that data provided to the Government by rights' holders was not subject to independent scrutiny and/or verification;
- 207.11. Less restrictive means of achieving the same objective were available.
208. **Fifthly**, there is an imbalance between the allocation of the costs and benefits of the measures in question. In particular:
- 208.1. For the reasons summarised in the witness statement of Mr. Heaney at [58], the overall cost-benefit analysis of the contested provisions fails to establish that there is an overall net benefit to society as a whole from the DEA 2010;
- 208.2. The benefits associated with the measures inure to the copyright owners, but they are not required to bear the full cost of the enforcement steps undertaken for their benefit.
- 208.3. The ISPs are instead subjected to onerous obligations which require them to endanger their relationship with their customers (who expect all their

communications to be private and respected, subject only to a Court order to the contrary);

208.4. The obligations also put the ISPs to significant expense, not all of which can realistically be recouped such as loss of customers and reputational harm. No provision has been made for a fair assessment of the fee to reflect this;

208.5. The contested provisions require BT and the ISPs to monitor and keep records of unlawful activity associated with a given IP address, regardless of whether or not the unlawful activity is taking place on a commercial scale. It therefore goes beyond the proportionality assessment inherent in Article 8 of the IPRE Directive.

209. **Sixthly**, less restrictive means of achieving the same objective are available. In particular:

209.1. There could be a more extensive education campaign;

209.2. The copyright owners could have greater recourse to the common law remedies available to them. The number of reported instances of the courts being used for civil actions is very small. See the Hunton and Williams updated report at Exhibit SM-28 at pp. 24 to 25;

209.3. Copyright owners could invoke to a greater extent and/or more effectively the 'take-down' procedures as set out in [67] of Mr. Heaney's witness statement;

209.4. The Government failed to analyse and take into account the results of the MOU trial, which put in place a less restrictive regime than the DEA 2010;

209.5. Other less restrictive means of combating the perceived problem have been set out in section 4 of the experts' report dated 1 July 2010.

210. It is also noteworthy that the EDPS in his Opinion dated 22 February 2010 (Exhibit SM-29) has also questioned whether other, less intrusive measures could combat the prevalence of unlawful file sharing. In this context, he has noted that:

210.1. The amendments made to the Universal Service Directive have not yet been tested to see whether they produce an appropriate restriction on unlawful file sharing. Any assessment of proportionality is premature until the efficacy of these less restrictive measures has been considered ([37] and [38] of the Opinion);

- 210.2. The IPRE Directive had only recently entered into force permitting Member States to combat commercial scale copyright infringement. Again, data on the efficacy of these measures is needed ([40]);
- 210.3. It was unclear whether any serious thought had been given to the possibility of alternative economic business models which would not need to involve the systematic monitoring of individuals;
- 210.4. Monitoring of the internet usage of individuals would only be proportionate where the “commercial scale criterion” was met. Monitoring in this context should be limited to specific, *ad hoc* situations, where well-grounded suspicions of copyright abuse on a commercial scale exist.
211. **Seventhly**, given the proper analysis of the cost-benefit analysis of the DEA 2010 regime, the restrictions on privacy and free expression entailed by the measures cannot be justified in the public interest.
212. Furthermore, it is clear that many other Member States have not felt the need to adopt such stringent measures as those adopted in the United Kingdom. The Study on Online Copyright Enforcement and Data Protection in Selected Member States, prepared by Hunton & Williams, Brussels, in November 2009 found that in relation to the legal systems of the six Member States analysed:⁴⁴
- 212.1. The processing of IP addresses by ISPs to pass on infringement warning notices is generally prohibited or subject to strict restrictions;
- 212.2. The general monitoring of P2P networks by rights holders resulting in the creation of a database of potential copyright infringers is usually prohibited;
- 212.3. The disclosure of P2P users’ identities by ISPs to judicial authorities in the context of criminal proceedings is generally authorised;
- 212.4. The disclosure of P2P users’ identities by ISPs to rights holder for civil enforcement is generally restricted by data protection law. In particular, ISPs may generally not disclose P2P users’ identities to rights holders outside the context of judicial review proceedings. Furthermore, Article 15(2) of the E Commerce Directive

⁴⁴ See Exhibit SM-27 to the witness statement of Simon Milner dated 5 July 2010.

envisaged the disclosure of unlawful activity only to the competent authorities and not to private individuals;

212.5. Generally, little thought had been given to the interaction between data protection rules and the implementation of the IRPE Directive;

212.6. The response of the different Member States threw up questions such as “how to apply the proportionality principle in practice and strike a fair balance between the various rights involved (such as the right to data protection and the right to property)”, given the absence of harmonisation at EU level.

(ii) The Defendant’s response

213. The Secretary of State has indicated in his pre-action protocol letter of response that the requirement for proportionality is inherently respected in the DEA 2010. That contention fails to meet the Claimants’ concern that the obligations imposed and/or envisaged by the DEA 2010 are inherently disproportionate. Furthermore, the Government’s analysis has proceeded on a flawed basis in any event. The Impact Assessment failed to take into account a number of material considerations and was otherwise *Wednesbury* unreasonable.

(iii) Relief

214. The Claimants seek a quashing order in respect of the contested provisions in the DEA 2010. In the alternative, declaratory relief to give effect to such findings as the Court may make is sought.

215. The Claimants will seek their costs of these proceedings if successful.

ANTONY WHITE QC

Matrix Chambers

KIERON BEAL

Blackstone Chambers

5 July 2010

ANNEX 1

Material provisions of the Digital Economy Act 2010

1. Section 3 of the DEA 2010 inserts a new section 124A into the Communications Act 2003 ('CA 2003'). It provides as follows:

“124A(1) This section applies if it appears to a copyright owner that—

(a) a subscriber to an internet access service has infringed the owner’s copyright by means of the service; or

(b) a subscriber to an internet access service has allowed another person to use the service, and that other person has infringed the owner’s copyright by means of the service.

(2) The owner may make a copyright infringement report to the internet service provider who provided the internet access service if a code in force under section 124C or 124D (an “initial obligations code”) allows the owner to do so.

(3) A “copyright infringement report” is a report that—

(a) states that there appears to have been an infringement of the owner’s copyright;

(b) includes a description of the apparent infringement;

(c) includes evidence of the apparent infringement that shows the subscriber’s IP address and the time at which the evidence was gathered;

(d) is sent to the internet service provider within the period of 1 month beginning with the day on which the evidence was gathered; and

(e) complies with any other requirement of the initial obligations code.

(4) An internet service provider who receives a copyright infringement report must notify the subscriber of the report if the initial obligations code requires the provider to do so.

(5) A notification under subsection (4) must be sent to the subscriber within the period of 1 month beginning with the day on which the provider receives the report.

(6) A notification under subsection (4) must include—

(a) a statement that the notification is sent under this section in response to a copyright infringement report;

(b) the name of the copyright owner who made the report;

(c) a description of the apparent infringement;

(d) evidence of the apparent infringement that shows the subscriber’s IP address and the time at which the evidence was gathered;

(e) information about subscriber appeals and the grounds on which they may be made;

(f) information about copyright and its purpose;

(g) advice, or information enabling the subscriber to obtain advice, about how to obtain lawful access to copyright works;

(h) advice, or information enabling the subscriber to obtain advice, about steps that a subscriber can take to protect an internet access service from unauthorised use; and

(i) anything else that the initial obligations code requires the notification to include.

(7) For the purposes of subsection (6)(h) the internet service provider must take into account the suitability of different protection for subscribers in different circumstances.

(8) The things that may be required under subsection (6)(i), whether in general or in a particular case, include in particular—

(a) a statement that information about the apparent infringement may be kept by the internet service provider;

(b) a statement that the copyright owner may require the provider to disclose which copyright infringement reports made by the owner to the provider relate to the subscriber;

(c) a statement that, following such a disclosure, the copyright owner may apply to a court to learn the subscriber's identity and may bring proceedings against the subscriber for copyright infringement; and

(d) where the requirement for the provider to send the notification arises partly because of a report that has already been the subject of a notification under subsection (4), a statement that the number of copyright infringement reports relating to the subscriber may be taken into account for the purposes of any technical measures.

(9) In this section “notify”, in relation to a subscriber, means send a notification to the electronic or postal address held by the internet service provider for the subscriber (and sections 394 to 396 do not apply).”

2. Section 4 of the DEA 2010 inserts a new section 124B into the CA 2003. That section imposes an obligation on ISPs to provide copyright infringement lists (‘CILs’) to copyright owners. It reads as follows:

“124B (1) An internet service provider must provide a copyright owner with a copyright infringement list for a period if—

(a) the owner requests the list for that period; and

(b) an initial obligations code requires the internet service provider to provide it.

(2) A “copyright infringement list” is a list that—

(a) sets out, in relation to each relevant subscriber, which of the copyright infringement reports made by the owner to the provider relate to the subscriber, but

(b) does not enable any subscriber to be identified.

(3) A subscriber is a “relevant subscriber” in relation to a copyright owner and an internet service provider if copyright infringement reports made by the owner to the provider in relation to the subscriber have reached the threshold set in the initial obligations code.”

3. Section 5 of the DEA 2010 inserts section 124C into the CA 2003. Section 124C(1) states that the obligations of internet service providers under sections 124A and 124B of the CA 2003 shall be called the “initial obligations”. Section 124C(2) requires Ofcom to approve an initial obligations code, but they may not do so unless it meets the criteria set out in section 124E of the CA 2003 (see section 124C(6)). By section 124C(10), the consent of the Secretary of State is needed for the approval of a Code or for its modification.

4. Section 124D CA 2003 (inserted by section 6 DEA 2010) requires Ofcom to make a Code under certain circumstances, but the obligation does not bite before the expiry of six months from the date of entry into force of the DEA 2010 or such longer period as the Secretary of State may direct.

5. Whether the Code is approved by Ofcom or adopted by it (see section 124D(4) CA 2003), section 124C(3) states that:

“The provision that may be contained in a code and approved under this section includes provision that—

(a) specifies conditions that must be met for rights and obligations under the copyright infringement provisions or the code to apply in a particular case;

(b) requires copyright owners or internet service providers to provide any information or assistance that is reasonably required to determine whether a condition under paragraph (a) is met.”

6. By sections 124C(4) and (5), it is envisaged that the Initial Obligations Code will make provision stipulating the number of notifications that can be made to an ISP by a copyright owner in a given period, make provision for payment of a fee and set a threshold at which the obligation to notify subscribers and maintain the CILs may be triggered.

7. Section 124E CA 2003 is inserted by section 7 of the DEA 2010. It sets down a series of minimum requirements for the Initial Obligations Code. It reads as follows:

“(1) The criteria referred to in sections 124C(6) and 124D(6) are—

(a) that the code makes the required provision about copyright infringement reports (see subsection (2));

(b) that it makes the required provision about the notification of subscribers (see subsections (3) and (4));

(c) that it sets the threshold applying for the purposes of determining who is a relevant subscriber within the meaning of section 124B(3) (see subsections (5) and (6));

(d) that it makes provision about how internet service providers are to keep information about subscribers;

(e) that it limits the time for which they may keep that information;

(f) that it makes any provision about contributions towards meeting costs that is required to be included by an order under section 124M;

(g) that the requirements concerning administration and enforcement are met in relation to the code (see subsections (7) and (8));

(h) that the requirements concerning subscriber appeals are met in relation to the code (see section 124K);

(i) that the provisions of the code are objectively justifiable in relation to the matters to which it relates;

- (j) that those provisions are not such as to discriminate unduly against particular persons or against a particular description of persons;
- (k) that those provisions are proportionate to what they are intended to achieve; and
- (l) that, in relation to what those provisions are intended to achieve, they are transparent.

(2) The required provision about copyright infringement reports is provision that specifies—

- (a) requirements as to the means of obtaining evidence of infringement of copyright for inclusion in a report;
- (b) the standard of evidence that must be included; and
- (c) the required form of the report.

(3) The required provision about the notification of subscribers is provision that specifies, in relation to a subscriber in relation to whom an internet service provider receives one or more copyright infringement reports—

- (a) requirements as to the means by which the provider identifies the subscriber;
- (b) which of the reports the provider must notify the subscriber of; and
- (c) requirements as to the form, contents and means of the notification in each case.

(4) The provision mentioned in subsection (3) must not permit any copyright infringement report received by an internet service provider more than 12 months before the date of a notification of a subscriber to be taken into account for the purposes of the notification.

(5) The threshold applying in accordance with subsection (1)(c) may, subject to subsection (6), be set by reference to any matter, including in particular one or more of—

- (a) the number of copyright infringement reports;
- (b) the time within which the reports are made; and
- (c) the time of the apparent infringements to which they relate.

(6) The threshold applying in accordance with subsection (1)(c) must operate in such a way that a copyright infringement report received by an internet service provider more than 12 months before a particular date does not affect whether the threshold is met on that date; and a copyright infringement list provided under section 124B must not take into account any such report.

(7) The requirements concerning administration and enforcement are—

- (a) that OFCOM have, under the code, the functions of administering and enforcing it, including the function of resolving owner-provider disputes;
- (b) that there are adequate arrangements under the code for OFCOM to obtain any information or assistance from internet service providers or copyright owners that OFCOM reasonably require for the purposes of administering and enforcing the code; and
- (c) that there are adequate arrangements under the code for the costs incurred by OFCOM in administering and enforcing the code to be met by internet service providers and copyright owners.

(8) The provision mentioned in subsection (7) may include, in particular—

- (a) provision for the payment, to a person specified in the code, of a penalty not exceeding the maximum penalty for the time being specified in section 124L(2);

(b) provision requiring a copyright owner to indemnify an internet service provider for any loss or damage resulting from the owner's failure to comply with the code or the copyright infringement provisions.

(9) In this section "owner-provider dispute" means a dispute that—

(a) is between persons who are copyright owners or internet service providers; and

(b) relates to an act or omission in relation to an initial obligation or an initial obligations code."

8. The DEA 2010 also lays down obligations concerning limitations on internet access. Section 9 of the Act inserts a new section 124G into the CA 2003. The material parts read as follows:

"(1) The Secretary of State may direct OFCOM to—

(a) assess whether one or more technical obligations should be imposed on internet service providers;

(b) take steps to prepare for the obligations;

(c) provide a report on the assessment or steps to the Secretary of State.

(2) A "technical obligation", in relation to an internet service provider, is an obligation for the provider to take a technical measure against some or all relevant subscribers to its service for the purpose of preventing or reducing infringement of copyright by means of the internet.

(3) A "technical measure" is a measure that—

(a) limits the speed or other capacity of the service 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.

(4) A subscriber to an internet access service is "relevant" if the subscriber is a relevant subscriber, within the meaning of section 124B(3), in relation to the provider of the service and one or more copyright owners.

(5) The assessment and steps that the Secretary of State may direct OFCOM to carry out or take under subsection (1) include, in particular—

(a) consultation of copyright owners, internet service providers, subscribers or any other person;

(b) an assessment of the likely efficacy of a technical measure in relation to a particular type of internet access service; and

(c) steps to prepare a proposed technical obligations code.

(6) Internet service providers and copyright owners must give OFCOM any assistance that OFCOM reasonably require for the purposes of complying with any direction under this section.

(7) The Secretary of State must lay before Parliament any direction under this section.”

9. Once a period of 12 months from the date of entry into force of the Initial Obligations Code has expired, the Secretary of State may by order impose a technical obligation on ISPs under a new section 124H if:
 - 9.1. Ofcom have assessed whether one or more technical obligations should be imposed on ISPs; and
 - 9.2. Taking into account reports that have been prepared and other relevant matters, the Secretary of State considers it appropriate to make an order.
10. Ofcom must, by virtue of section 124I CA 2003 (inserted by section 11 DEA 2010), make by order a technical obligations code for the purpose of regulating any technical obligations while any are in force. The prescribed contents of such a technical obligations code are set out in a new section 124J CA 2003 (inserted by section 12 DEA 2010):

“(1) The criteria referred to in section 124I(4) are—

- (a) that the requirements concerning enforcement and related matters are met in relation to the code (see subsections (2) and (3));
- (b) that the requirements concerning subscriber appeals are met in relation to the code (see section 124K);
- (c) that it makes any provision about contributions towards meeting costs that is required to be included by an order under section 124M;
- (d) that it makes any other provision that the Secretary of State requires it to make;
- (e) that the provisions of the code are objectively justifiable in relation to the matters to which it relates;
- (f) that those provisions are not such as to discriminate unduly against particular persons or against a particular description of persons;
- (g) that those provisions are proportionate to what they are intended to achieve; and
- (h) that, in relation to what those provisions are intended to achieve, they are transparent.

(2) The requirements concerning enforcement and related matters are—

- (a) that OFCOM have, under the code, the functions of administering and enforcing it, including the function of resolving owner-provider disputes;
- (b) that there are adequate arrangements under the code for OFCOM to obtain any information or assistance from internet service providers or copyright owners that OFCOM reasonably require for the purposes of administering and enforcing the code; and
- (c) that there are adequate arrangements under the code for the costs incurred by OFCOM in administering and enforcing the code to be met by internet service providers and copyright owners.

(3) The provision made concerning enforcement and related matters may also (unless the Secretary of State requires otherwise) include, in particular—

- (a) provision for the payment, to a person specified in the code, of a penalty not exceeding the maximum penalty for the time being specified in section 124L(2);
- (b) provision requiring a copyright owner to indemnify an internet service provider for any loss or damage resulting from the owner's infringement or error in relation to the code or the copyright infringement provisions.

(4) In this section "owner-provider dispute" means a dispute that—

- (a) is between persons who are copyright owners or internet service providers; and
- (b) relates to an act or omission in relation to a technical obligation or a technical obligations code."

11. Section 13 of the DEA 2010 provides for subscriber appeals. An initial appeal is envisaged, together with a further right of appeal to the First-Tier Tribunal in relation to an appeal concerning the imposition of technical obligations. Section 124K(3) CA 2003 sets out a non-exhaustive list of grounds of appeal, including: (a) that the apparent infringement to which the report relates was not an infringement of copyright; and (b) that the report does not relate to the subscriber's IP address at the time of the apparent infringement. Sections 124K(5) and (6) CA 2003 now provide as follows:

"(5) The code must provide that an appeal on any grounds must be determined in favour of the subscriber unless the copyright owner or internet service provider shows that, as respects any copyright infringement report to which the appeal relates or by reference to which anything to which the appeal relates was done (or, if there is more than one such report, as respects each of them)—

- (a) the apparent infringement was an infringement of copyright, and
- (b) the report relates to the subscriber's IP address at the time of that infringement.

(6) The code must provide that, where a ground mentioned in subsection (3) is relied on, the appeal must be determined in favour of the subscriber if the subscriber shows that—

- (a) the act constituting the apparent infringement to which the report relates was not done by the subscriber, and
- (b) the subscriber took reasonable steps to prevent other persons infringing copyright by means of the internet access service."

12. A person hearing subscriber appeals may make an award of compensation or costs and make appropriate directions concerning technical measures. See sections 124K(7) to (9) CA 2003.

13. Section 14 of the DEA 2010 provides for a new section 124L of the CA 2003. This applies by cross-reference the terms of sections 94 to 96 CA 2003, permitting Ofcom to

impose penalties not exceeding £250,000 on individuals in respect of any of the following:

- 13.1. A contravention of an initial obligation;
- 13.2. A contravention of a technical obligation;
- 13.3. A contravention of the obligation imposed by section 124G(6) to give Ofcom any assistance it reasonably requires.

14. Section 15 DEA 2010 has introduced an enabling section in section 124M of the CA 2003, empowering the Secretary of State by statutory instrument to make an Order addressing the question of costs-sharing or costs allocation arising from costs incurred in complying with the initial obligations or any technical obligation.

15. Section 124N (inserted by section 16 DEA 2010) sets out a series of definitions. Internet service provider is defined as a person who provides an internet access service. That service is in turn defined as an “electronic communications service that is: (a) provided to a subscriber; (b) consists entirely or mainly of the provision of access to the internet; and (c) includes the allocation of an IP address or IP addresses to enable that access.” Definitions are also given for “IP address” and “subscriber.”

16. Section 17 DEA 2010 contains provisions which empower the Secretary of State to make Regulations concerning the grant of injunctive relief by a Court against an ISP to prevent its service being used to give access to a particular internet location. This is referred to as a blocking injunction. The Court must be satisfied that the location has been, is being or is likely to be used for or in connection with an activity that infringes copyright. Sections 17(4) and 17(5) set out the substantive content that the Regulations must contain:

“(4) The regulations must provide that a court may not grant an injunction unless satisfied that the location is—

- (a) a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright,
- (b) a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or
- (c) a location which has been, is being or is likely to be used to facilitate access to a location within paragraph (a) or (b).

(5) The regulations must provide that, in determining whether to grant an injunction, the court must take account of—

- (a) any evidence presented of steps taken by the service provider, or by an operator of the location, to prevent infringement of copyright in the qualifying material,
- (b) any evidence presented of steps taken by the copyright owner, or by a licensee of copyright in the qualifying material, to facilitate lawful access to the qualifying material,
- (c) any representations made by a Minister of the Crown,
- (d) whether the injunction would be likely to have a disproportionate effect on any person's legitimate interests, and
- (e) the importance of freedom of expression.”

17. Pursuant to sections 47(1) and (2) DEA 2010, sections 124A and 124B of the CA 2003 come into force on 8 June 2010. Sections 124C to 124E, 124M and 124N all come into force on 8 April 2010. The remainder of the relevant provisions identified above come into force on 8 June 2010.