



**Online Infringement of Copyright and the Digital
Economy Act 2010
Draft Initial Obligations Code**

**Ofcom Consultation document
response from BT**

30 July 2010

Executive Summary

BT is pleased to offer a response to this Consultation, and recognises that Ofcom had comparatively little time to produce the document following the passage of the Digital Economy Act (DEA) in early April.

BT's comments are made without prejudice to our ongoing application for Judicial Review of certain sections of the DEA. As Ofcom is aware, BT is currently in the process of questioning the validity of these provisions in this area through the courts. Our comments in this response should therefore not be considered as suggesting that BT agrees in any way that the obligations imposed on Ofcom to produce a Code are enforceable under EU law.

BT has some significant concerns about the approach Ofcom proposes to take in fulfilling its initial obligations under the DEA's provisions on online copyright infringement. Since the text of the Code which emerges will be based on the principles and policy ultimately adopted by Ofcom, this response focuses on these aspects rather than commenting on the detailed text of the draft Code in Annex 5 of the Consultation or every question posed in detail.

- Ofcom has not given proper time and attention to squaring its responsibilities under the DEA with its other duties under the Communications Act in particular for promoting competition and protecting consumers.
- Ofcom's proposal to exclude mobile ISPs from the provisions of the Code and yet include Wi-Fi services is unfair, disproportionate and most importantly is without substantive, evidence-based explanation. We provide compelling reasons for excluding Wi-Fi at Annex 1 of this response. If Ofcom decides, nonetheless, to include Wi-Fi services within scope, the logical corollary is that mobile ISPs should be included too.
- Ofcom's proposal that copyright owners should commit to volumes of CIRs two months in advance of ISPs being obliged to receive and process those CIRs is unreasonable given the significant systems, process and customer impacts of different scenarios. This lead time should be extended to six months.
- Ofcom should look to establish an interim code for the 'soft launch' phase of the notifications regime including an interim approach to a threshold for ISP inclusion. The soft launch period will provide all parties with an opportunity to iron out teething problems in the Code's application and allow Ofcom to take a more informed approach to the scope of the Code based on actual and potential CIRs.
- Ofcom should avoid giving the impression that CIRs and particularly the IP address and time/date stamp within a CIR constitute evidence of wrongdoing.
- Ofcom should apply more rigour to the process of subscriber 'appeals' in particular with reference to its responsibilities to protect consumers.

1. Ofcom's DEA and other Communications Act responsibilities

30 July 2010

The way the Consultation has been produced gives rise to concerns that Ofcom is rushing into dealing with its DEA functions on the basis of the previous Government's approach during the Bill phase and that Ofcom is inclined to prioritise and make policy choices for implementation accordingly. A better approach would be to take a fresh, independent regulator's look at an approach to the Code which maximises coherence and consistency with Ofcom's established existing Communications Act 2003 (CA) roles and modus operandi as well as with forthcoming implementation of the EU Communications Package Directives in the UK.

The DEA creates a wholly new area of regulation by Ofcom. In the last Government's rush to get the legislation passed, many fundamental issues of how this new area of regulation would sit with and interrelate with Ofcom's existing fields of regulation under the CA were not examined and clarified.

The CA sets out Ofcom's principal duty - to promote and further the interests of citizens in relation to communications matters and of consumers in relevant markets, where appropriate by promoting competition. It also recognises that conflicts may arise when Ofcom carries out different functions, which ones take priority if that arises (including the status of functions arising under EC obligations) and how conflicts are to be resolved.

Ofcom's role under the CA includes regulatory and competition functions to facilitate undistorted competition in communications markets. The Consultation refers to Ofcom's role in relation to promotion of citizen and consumer interests but does not refer to or clarify how its competition activities interrelate with its DEA functions and indicate how they might be applied. This omission is stark given that Ofcom's proposals, such as the qualifying threshold test for ISPs and statements about its "requirements" and "expectation" for changes to ISPs business models and contracts for provision of service to them from upstream communications providers, have obvious potential to distort competition in communications markets (leading to positive or negative discrimination against customers of affected communications providers and ISPs).

It is essential that Ofcom's proposals to give effect to measures introduced in the DEA provide similar clarity about its new DEA functions. Everyone needs to understand what the basic ground rules of the revised CA playing field are so they are clear what can be legitimately required of them and can form legitimate expectations on issues such as dispute resolution mechanisms, enforcement and sanctions.

If Ofcom were to conduct a systematic assessment of the touch points of the DEA with the CA, applying its customary rigour and evidence-based analysis, and feed that assessment through into Code development, it is likely to produce a better Code than the current proposals. It should lead to a Code that engenders greater all-round confidence that it is fair, balanced, transparent, minimises potential competitive distortions and is non-discriminatory .

BT's concerns align with the following points made in the Second Report of the House of Lords Delegated Powers & Regulatory Reform Committee¹ issued during the passage of the Digital Economy Bill:

9. A reasonable indication of the things which a code is likely to contain is apparent from new sections 124C(3), (4) and (5) and (in the case of a code made by OFCOM) 124D(4). Additionally, a code must meet the criteria specified in new section 124E. So, for example, the code must contain provisions about enforcement and those provisions may include provision for civil penalties. The Government's memorandum makes it clear that much of this is based on sections 52 to 55 and 120 to 125 of the 2003 Act which are about customer interests conditions and a code for premium rate services. Inevitably, because of the different subject matter, there will be differences between the provisions of sections 52 to 55 and 120 to 125 of the 2003 Act on the one hand and the new provisions in this Bill on the other.

10. It appears to us that, if the House accepts that OFCOM should have a role in controlling infringement of copyright, the contents of the code are generally an appropriate matter for delegated legislation. However, the analogy drawn in the Government's memorandum between these powers and the powers given to OFCOM in the 2003 Act relating to customer interests conditions and premium rate services holds good only to a certain extent. The powers in the 2003 Act are aimed at regulating the conduct of those providing a communications network or service, but the powers in this Bill are aimed at ultimately regulating the conduct of subscribers to a service (i.e. consumers).

2. Copyright Owner Issues

Demand forecasts and costs

The DEA is in place to benefit copyright owners. They are the source of CIRs and already engage in investigation, detection and in sending notices of alleged copyright infringement by internet users to ISPs on a scale which they determine and at costs which are known to them.

There is a strong impression, however, from the Consultation (and in Ofcom's other activities relating to DEA implementation) that Ofcom is fighting shy of obtaining best first-hand information from copyright owners in order to develop the Code.

The failure to do so means that ISPs are currently unable to plan what to put in place to handle CIRs and CILs and the "customer wrap" around that, but face pressure to do just that within a short timescale. This failure also means that Ofcom is preventing itself from acquiring the very information which would

¹ <http://www.publications.parliament.uk/pa/ld200910/ldselect/lddelreg/24/24.pdf>

30 July 2010

best enable it to bring into place thresholds for identifying which ISPs should be subject to obligations on a basis that meets or approximates most closely to the requirements of the DEA. Ofcom should be more demanding of copyright owners and those organisations should have no problem disclosing their intended level of demand for CIRs several months ahead. BT suggests that the Code should specify that copyright owners commit to a six-month lead time on the volume of CIRs they will submit to each ISP.

ISPs and internet users are entitled to be satisfied that the implementation of the DEA through the Code is fair, balanced and transparent. The round-about way which Ofcom is currently using to assess volumes of CIRs and costs has the effect of expanding from the outset potential demand for CIR processing and creates the opportunity for copyright owners to game the system to acquire cost subsidies from ISPs and their customers for their detection and notification activities.

In addition, Ofcom is failing to use (or is not using transparently) information that copyright owners can directly provide on their current (unsubsidised by ISPs) criteria and costs for detection and notice-sending. It is apparent that each of the film and music industries chooses to detect unlawful file-sharing associated with a proportion of their portfolios of copyright works at any one time and not the full portfolio at all times. Copyright owners also regularly change the specific titles to be followed, based on their evaluation of which they consider to be of commercial value at a particular time.

It is not justifiable to use the DEA and the cost subsidisation of detection and notification of copyright owners that it might provide, as a tool to broaden and expand the “market” for detection and notifications.

There is no rationale to stray from the normal principles for dealing with supply and demand of services, i.e. in this case copyright owners are seeking supply of a service from ISPs and it is incumbent on them to provide realistic forecasts of actual demand for that service to which “service supplier” ISPs respond. However, given that the obligations imposed on ISPs under the DEA are not activities that they would engage in as part of their business activities to serve customers it is economically sound and rational to ensure that ISPs should not and do not over-invest in service capabilities, in particular where the risk of unrecoverable costs lies with them.

The proper approach should be that ISPs’ capabilities are demand-led (with realistic lead times) from the volumes that copyright owners who propose to use the service can justify as being proportionate and not excessive. Without this there is a real danger that ISPs will over- or under- invest in technology, systems and headcount to deliver their DEA initial obligations.

Ofcom should ensure that the Code and assurance requirements for copyright owners prevent them from discriminating in favour or against individual ISPs.

Robustness, accuracy and inferences from IP address information gathered by copyright owners

The foundation of the DEA is the allegations of copyright infringement made by copyright owners. It is, therefore, essential that Ofcom takes an active, ongoing role to establish exactly how copyright owners are conducting their investigations and the limits of their claims in terms of accuracy and robustness of identification of IP addresses involved in suspected copyright infringement. The Code will not be fair to ISPs and internet users and take account of due process sufficiently if this is not done.

Ofcom's approach to establishing the role and relationship of the detection companies and copyright owners, the limitations on the techniques used, the probability of the information generated being unreliable², etc. must be more rigorous and objective than currently proposed.

BT shares the perception of many others – technical experts, consumer and citizen groups alike – that there is a tendency for copyright owners to overstate the evidential quality of the information they produce and the degree to which courts accept such information as proof of copyright infringement. For example

- the judicial systems of a number of countries do not accept that the IP address information acquired by copyright owners through their detection methods are reliable evidence that proves a particular IP address was indeed involved in an activity in breach of copyright;
- the current acceptance in English courts of information provided by copyright owners as a basis on which Norwich Pharmacal disclosure orders may be granted does not entail that information being assessed by the court as proof of copyright infringement having occurred or being attributable to the person whose name is the subject of disclosure. In a recent Australian³ case in which copyright owners brought copyright infringement proceedings against an ISP, the judge was very clear that he could not ascertain the relationship between the copyright owners and the organisation, AFACT, which they used to detect copyright infringement.

There needs to be a clear understanding by all parties involved in the DEA – whether as ISP, subject of an infringement allegation, regulator or hearer of appeals – that the fact that an IP address is picked up by copyright owners detection methods is not, of itself, proof that the IP address or the person that it was allocated to was involved in copyright infringement activity. The information goes no further than being an indication that a particular IP address may have been involved.

² <http://www.piercelaw.edu/assets/pdf/release-mavis-case-expert-report.pdf>
<http://arstechnica.com/old/content/2008/06/study-paints-grim-picture-of-automated-dmca-notice-accuracy.ars>

³ <http://www.austlii.edu.au/au/cases/cth/FCA/2010/24.html>
Roadshow Films Pty Ltd v iiNet Limited (No.3) [2010] FCA 24, paragraphs 80 - 82

Ofcom should re-evaluate its current approach to copyright owners and take steps to ensure that the Code does not operate such that:

- citizens and consumers in the UK will face greater adverse consequences from being the subject of copyright infringement allegations under the DEA than they would face from responding to allegations based on the same information in an English court or compared to their counterparts in many other countries;
- ISPs are required to impute that infringement allegations are stronger than they are. Their exposure to risks and liabilities for acting on such information are unjustifiably increased by doing so. This also has significant consequences for the tone and content of the notifications and information they provide to their customers.

The current proposals are inadequate to assess objectively the nature of the IP address-based allegations of infringement which underpin the DEA. It is inevitable that Ofcom's assessment of the proportionality of any of the activities which are set in train by those allegations, e.g. for internet access providers and for subscribers, will not be soundly-based.

Ofcom's approach shows that it has failed to appreciate the significant and manifest differences between the existing limited way in which ISPs may be dragged into copyright infringement enforcement activities to assist copyright owners compared to the extensive requirements being placed on ISPs under the DEA. Under the former an ISP provides an IP address match if there is one in the ISP's records to copyright owner on the order of a court; copyright owner corresponds with name disclosed. Under the latter an ISP will be required to undertake prolonged and active processing of allegations without any judicial involvement, and which extends to the creation, maintenance and disclosure of lists dealing with confidential data and content of communications in which it is intrinsic that those placed on the lists are treated as having engaged in wrongdoing. The ISP will have to engage in an extended communication programme with customers so identified.

3. DEA Interpretation

Ofcom's proposals on a number of key issues are justified by reference to its reading of the DEA, Bill documents and presumptions. Some of these are strained, inconsistent or unjustified. There are alternative interpretations which would lead to different Code outcomes from those proposed in the Consultation which are reasonable and preferable. We indicate some key issues where we consider that fairer, clearer and more certain outcomes could be achieved by adopting an alternative approach.

Changes to ISPs business models

Various statements in the Consultation indicate that Ofcom "requires" and, or "expects" ISPs who may be subject to DEA obligations (in order to acquire IP data that they do not possess for the sole purpose of making themselves subject to DEA requirements) to:

30 July 2010

- change the terms and conditions on which they do business with other communications providers (paragraph 3.27);
- change the internet access services they offer (paragraph 3.28).

We do not see anything in the DEA or Bill documents that suggests that such a far-reaching approach is intended. There are no regulatory or economic assessments suggesting this possibility was envisaged and debate on the Bill did not indicate this. Throughout the passage of the DEA, we cannot see that it has been suggested that a fixed ISP (such as one who participated in the P2P MoU) who is unable to produce from its records a subscriber match to an IP address submitted to it by a copyright owner, is under any obligation to make changes to eliminate that situation from recurring.

A court would not require a communications provider to positively generate the means to acquire data in order to put the court in a position to make a disclosure order on that provider. More generally, it appears to us that courts do not require ISPs to change their legitimate business models for the purpose of accommodating IPR enforcement activities

Qualifying Threshold

We do not consider that there is any basis in the DEA or otherwise for setting thresholds except by reference to CIRs. We do not agree that Ofcom's power under section 1124D (5) (h) can be relied on in the way Ofcom contends to introduce a new and different test from the one explicitly set out in the DEA. We comment on this further in our detailed responses below and in particular on the exclusion of mobile broadband providers and the implications this has for Wi-Fi providers in Annex 1.

Applying definitions and tests

Ofcom needs to clarify the factors that are involved in its assessment of what would be disproportionate, fair, reasonable and balanced. We agree that costs are an obvious and important factor, but costs are not the only factor.

Some other factors which Ofcom should take into account are disproportionality, or other unfairness or impracticalities arising from whether the persons involved in offering internet access provision are:

- making it available as part of its business or in a non-commercial capacity, e.g. for education or public purposes
- making it available as an adjunct to a different primary business which is not related to provision of electronic communications as such, e.g. to purchase goods and services, hotel and leisure service provision
- can really be characterised as making it available pursuant to "an agreement" to provide services if one can only "imply" that an agreement exists.

Ofcom should revise its current approach which is calculated to produce over-reaching application of the DEA to all kinds of internet access providers and

30 July 2010

users, such as businesses or Wi-Fi network providers of any kind and in any capacity.

Technology and user behaviour

Ofcom also specifically needs to take into account the realities of technological development and evolution of the internet, the applications that are used and evolve and user behaviour. These are not controlled by the internet service providers who may fall within scope of the DEA.

It is not appropriate to subsume such issues simply into a “costs issue”. First, because all these issues are not amenable to being addressed by unilateral action by one or more ISPs in the UK, irrespective of the amount of development and resources they expend on these issues.

The issue is primarily one of whether what ISPs may be asked to do under the Code will be effective to any degree or at all. The essential question is the proportionality of:

- obliging ISPs to take on-going and continuous action to change internet experience and technologies. i.e. engage in an arms race that cannot be “won” ; and
- to elevate the DEA requirements on ISPs above any other consideration relevant to their operations.

4. Privacy and Data protection

ISPs will be required by the Code to undertake activities which systematically impact on the privacy, data protection and confidentiality of customers and internet users generally. BT has a well-founded expectation that many people will have concerns leading to high volumes of queries and complaints arising on these grounds.

ISPs also require direct guidance from the ICO to ensure that systems are specified properly in terms of security, access, authorisation, disclosure aspects and data retention periods. All the documents we have seen to date in terms of costs exercises before and after the passage of the DEA fail to recognise the significant implications for system design and costs these issues pose.

We are clear from recent ECJ case law and pronouncements of national and EU DP regulators that

- processing of traffic data is seen as highly intrusive;
- any processing of data that relates to content of communications by internet access providers is highly controversial and fraught with legal difficulties;
- queries have been raised about the legitimacy of private sector entities - copyright owners or internet service providers – processing the data

30 July 2010

which emanates from P2P file-sharing activities for copyright enforcement purposes;

- queries have been raised about the justification for retention duration periods of more than 6 months for internet traffic data under the Data Retention Directive.⁴

The Data Retention Directive relates to data retained for serious crime purposes for disclosure to appropriate authorities. In contrast, under the DEA, ISPs will be holding more than just traffic data, the data will be disclosable to private entities (e.g. copyright owners and their associates) and proposals appear to assume retention periods of no less than 12 months

It is imperative, therefore, that the relevant regulator in this field, which is the ICO and not Ofcom, provides explicit guidance and advice to enable ISPs to understand and manage their risks and liabilities. BT will not have the means to address and make relevant and reliable representations to its customers and end users and deal with their queries and complaints adequately if such guidance is not directly available from the ICO.

Ofcom should also take specific account of the extent to which requirements proposed by the Code, insofar as it envisages the introduction of or an increase in monitoring and other intrusion by ISPs in relation to their subscribers and also by a subscriber in relation to users of the relevant internet connection, are likely to be disproportionate on data protection and privacy grounds.

5. Subscriber Appeals

Fairness and due process demands that anyone receiving an allegation must be able to contest it. BT, therefore, fully supports a procedure that enables them to do so. The regime created by the DEA fundamentally alters the nature of the legal and contractual relationships which currently exist in relation to internet service provision. The paramount importance of providing adequate checks and balances for subscribers, so that they can challenge infringement allegations made against them, was recognised by Parliament and is fully recognised by BT too.

BT has, however, a number of concerns of principle regarding the approach taken which stem from issues raised by application of the DEA in the way proposed by Ofcom in its proposals.

We have already referred to concerns that there appears to be an assumption that being the subject of a notification carries the connotation of wrongdoing and being involved in it. We make more detailed comments in our response to Q6 below.

⁴http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp172_en.pdf

30 July 2010

The relevant provisions of the DEA were introduced late and somewhat incoherently during the passage of the Bill because of the previous Government's failure to appreciate the significance of the issues involved from the outset. They are convoluted, complex and many aspects are unclear. We recognise the pressured timetable that Ofcom is currently working under, but the proposals in the Code and the principles informing their application must be developed and explained much more than the present, essentially superficial approach in the Consultation. In particular this is needed

- to show that Ofcom fully appreciates the implications of "subscriber appeals" for all aspects of the DEA
- as tangible expression of Ofcom's duty to promote citizen and consumer interests
- clarify where there are or may be conflicts between the new DEA provisions and pre-existing provisions of the CA and how Ofcom will reconcile or otherwise address them.

The language of "appeal" and "Appeal Body" is included in the DEA. There should be recognition, however, that in the situation when a person is contesting an allegation the process is not properly characterised as an "appeal". An appeal is where a person is the subject of a decision of a tribunal and the person wishes to challenge that decision. Here, what happens is merely that one person wishes to challenge the action of another: neither a copyright owner nor an ISP is a tribunal making a decision within the normal application of the term "appeal".

The DEA introduces provisions which appear to make some very striking changes on matters such as what constitutes copyright infringement, who might be held responsible for infringement occurring, duties on persons to prevent/ deter copyright infringement from arising. These include:

- a new obligation on ISPs to provide advice or information to subscribers about steps to protect an internet service from unauthorised use
- a requirement for a subscriber to show that it took reasonable steps to prevent other persons infringing copyright by means of the internet access service in order to succeed in any subscriber appeal.

The Code leaves unanswered the question of what happens in the case of a subscriber seeking to assert that they had not infringed copyright having received a Notification Letter, but had not taken previous steps to secure their internet connection. The failure by that subscriber to take positive action in circumstances where he may have had no prior knowledge of the efficacy of doing so appears to place such a subscriber at an immediate disadvantage in the appeal proceedings. The fact is that subscribers may only get to see this information for the first time when they receive the Notification Letter which they want to appeal, by which time it is too late to assist them to clear their name. It also places the burden on ISPs to interpret what is meant by 'reasonable steps'.

30 July 2010

The Consultation offers no information on Ofcom's views and intentions on interpretation, application and enforcement of these provisions. There is no certainty of any kind for communications providers, ISPs, and subscribers of all types (businesses, institutions, consumers).

6. Administration, enforcement disputes and information gathering

There are many practical, procedural and legal issues of significance and impact lurking in these areas. We have stated above that we are unclear on many aspects of how the new DEA and existing CA provisions and Ofcom's approach will be applied in relation to communication providers, internet users and copyright owners.

While so much of the regime is unclear we are unable to conclude that Ofcom's approach strikes the balance that it sets itself in paragraph 8.5 of the Consultation. The full panoply of enforcement and other powers should not be brought into force immediately on the making of a Code.

Guidelines and principles for enforcement, information gathering etc. need to be developed first. When developing them Ofcom must specifically address how these aspects are to be applied fairly and proportionately. It is inevitable that difficult conflicts will arise for communications providers/ISPs between meeting certain DEA requirements and meeting other regulatory/legal requirements under CA or other legislation, or customer and consumer interests.

In view of the uncertainty on numbers and processes, and our concerns raised above and in the detailed responses to Ofcom's questions, we strongly recommend that the Code is implemented in a phased way. We need to fully understand the volumes of CIRs before we can ensure our systems are sufficiently robust. As the focus to date has mainly been on residential customers, we would also propose that the first phase only covers this group. It is only once there is a clearer understanding of how it will all work and of the CIR levels that business subscribers should be brought into scope if this is felt to be necessary (unless a low level of infringement can be shown).

BT's view is that a phased introduction would allow a better all round experience to be developed for copyright owners, ISPs and subscribers. It would also provide evidence on which any Code could be developed further by Ofcom, taking into account all the relevant duties and obligations of transparency, proportionality and non discrimination.

30 July 2010

RESPONSE TO SPECIFIC QUESTIONS

Question 3.1: Do you agree that Copyright Owners should only be able to take advantage of the online copyright infringement procedures set out in the DEA and the Code where they have met their obligations under the Secretary of State's Order under section 124 of the 2003 Act? Please provide supporting arguments.

It is extremely important for all those affected by the operation of the intrusive new requirements introduced by the DEA that the persons able to invoke it for their benefit are able to demonstrate their willingness to abide by requirements in it which are intended to help make the DEA regime fair, balanced and proportionate.

Cases involving copyright owners in the UK and elsewhere, illustrate that copyright owners are apt to be extremely aggressive in their accusations against those they consider to be infringing and those providing evidence to support defendants against allegations. The passage of the DEA has also been accompanied by much concern amongst Parliamentarians as well as by citizen and consumer groups about perceived bullying of subscribers and inaccuracies in the assertions made by some copyright owners and those acting on their behalf when pursuing enforcement of copyright.

Data protection and privacy concerns about copyright owners detection and processing of data and about disclosure of data to them and parties associated with them (trade organisations, detection agencies) are also well-aided.

There should be no question arising of ISPs being required to undertake activities under the DEA or of consumers and citizens facing allegations unless demonstrable and enforceable commitments are first made by copyright owners.

We remain concerned that it is not clear which requirements on copyright owners are enforceable under Ofcom's DEA functions or other CA duties and powers and which are not. There is no discussion in the Consultation about dealing with indemnities from copyright owners to ISPs. However, as these are intended to provide a safeguard to ISPs to recompense them for liabilities which ISPs may face as a result of copyright owners it is very important for fairness, balance and transparency that copyright owners are required to give meaningful indemnities, i.e. ones that properly enable ISPs to recover losses. Ofcom's approach should include proposals for how that can be facilitated and, or achieved through the Code and relevant Order.

Question 3.2: Is two months an appropriate lead time for the purposes of planning ISP and Copyright Owner activity in a given notification period? If a notification period is significantly more or less than a year, how should the lead time be varied? Please provide supporting evidence of the benefits of an alternative lead time.

Any implementation involving major systems across a whole product set or customer base inevitably requires a long lead time to ensure effective deployment. In the P2P MoU, different ISP operators started “coming on stream” at different times and the conditions and times for ramping up to the maximum volumes processed under the MoU varied between them too. It was possible to implement in a relevant timescale because the volume of notifications was specified well in advance of the MoU being signed and also the number of copyright entities providing them was specified and did not change. Furthermore every ISP involved adopted a largely manual handing process. The lead time involved was no less than two months. The variations were not attributable to any “efficiency” or “lack of efficiency” by a particular operator. The facts are that their systems and products vary considerably.

The evidence, therefore militates against proceeding on a single “big bang” start date involving many ISPs, whether they were previously involved in the P2P MoU or not. If there are ISPs, such as those with well-established content interests, who are on a faster track for implementation than others, then provided their costs do not form the basis for calculating other ISPs costs, perhaps they should press ahead and provide some of the road-testing for the DEA that is currently lacking.

The cost SI consultation envisaged ISPs and copyright owners dropping in and out of the Code. Ofcom’s qualifying threshold test also contemplates ISPs coming into the Code as and when Ofcom change criteria. This is a significant factor complicating the regime. If Ofcom and the Government are, nevertheless, already committed to implementation on this basis, then they can have no reason for insisting on a big bang “start-up”

In BT’s case, it is not possible to answer this question without better understanding the anticipated volumes of reports that will be submitted by copyright owners. If volumes are at low levels, then it might be possible to support this timeframe using a manual process and increasing FTE proportionately. Any significant volume will require systems developments which will require a significantly different lead time. This will be the case even at the volume levels in the P2P MoU because the processing and notification requirements under the DEA are significantly different. It is not possible to identify the length of this lead time at this point without first clarifying the many other issues being raised in this response. In the interim we suggest that Ofcom should set a lead time of six months.

Question 3.3: Do you agree with Ofcom’s approach to the application of the Code to ISPs? If not, what alternative approach would you propose? Can you provide evidence in support of any alternative you propose?

Question 3.4: Do you agree with the proposed qualification criteria for the first notification period under the Code, and the consequences for coverage of the ISP market, appropriate? If not, what alternative

30 July 2010

approaches would you propose? Can you provide evidence in support of any alternative you propose?

Question 3.5: Do you agree with Ofcom's approach to the application of the 2003 Act to ISPs outside the initial definition of Qualifying ISP? If you favour an alternative approach, can you provide detail and supporting evidence for that approach?

Question 3.6: Do you agree with Ofcom's approach to the application of the Act to subscribers and communications providers? If you favour alternative approaches, can you provide detail and supporting evidence for those approaches?

See our comments elsewhere in this response and in Annex 1 dealing with mobile and Wi-Fi aspects specifically

In paragraph 3.10 of the Consultation on the Code, Ofcom states it has considered three questions in determining the application of the Code to ISPs which are as follows:

- should the Code initially apply to both fixed and mobile ISPs;
- if only fixed, what coverage of fixed ISPs would be proportionate;
- the approach they should adopt to discourage churn to ISPs out of scope of the Code.

Ofcom has not obtained any CIR numbers on the basis of which to set thresholds at the moment, but this does not justify the adoption of a different test based on subscriber numbers of ISPs instead. This threshold is arbitrary and will lead to market distortion.

While we accept that the ISPs who would be covered in this threshold serve a large proportion of the residential broadband market, closer analysis is required of the impact on the business sector. As many of our business broadband competitors are smaller players, we believe the 400k threshold could lead to customers moving to a business ISP who is not required to comply with the Code. Business subscribers in particular may find it onerous to identify the person who allegedly infringed copyright and so may be tempted to move to an ISP outside the scope of the Code.

While we accept that Ofcom does not want to impact disproportionately on small ISPs we would question if this would be the case if the costs are appropriately allocated to copyright holders and so would question the need for any threshold for fixed ISPs at this stage. As more information is gathered on infringement reports then threshold criteria could be assessed going forward and if an ISP can demonstrate a low level of infringement it should be able to fall out of scope.

Further, we would question Ofcom's ability in any event to use its general power under section 124(5)(h) of the 2003 Act to create a new mechanism for calculating a threshold based on the number of subscribers an ISP has when the DEA makes provision only for a threshold based on the number of CIRs

received by that ISP. The general power granted is in relation to regulating the initial obligations which already exist, and does not extend to rewriting the DEA to provide for an alternative method of determining which ISPs the new legal obligations will fall on, when the primary legislation did not anticipate this.

Surely the correct interpretation of the DEA is for an initial period in which the number of CIRs received by all ISPs is assessed before making any judgment about who the Code should apply to. Ofcom's rationale for making its decision about who is or is not in scope at the outset of the Code is based on evidence provided by copyright owners which has neither been shared with the ISPs nor to our knowledge empirically tested for accuracy and completeness. It does not take account of the different technologies employed in the provision of internet access, their users, or their alleged propensity to file-share.

Many entities which would not have been regulated by Ofcom in respect of provision of communications services prior to DEA might now be regulated. The issue arises, therefore, if that also renders such entities subject to Ofcom, CA and EC communications regulation more generally. Ofcom must take the trouble to explain and set out clearly the extent to which that is indeed a consequence and the implications. It is not clear to us that Ofcom's proposed approach to interpretation of new definitions in the DEA, taken together with the application of pre-existing definitions in the CA as well as definitions arising under existing and forthcoming EC communications law, do fit together coherently. Various propositions in Section 3 appear to be inconsistent, contradictory or could be perceived as out-of-kilter with normal expectations of businesses, citizens and consumers alike and to carry significant potential to give rise to unexpected and unintended consequences.

Question 4.1: Do you agree with the proposed content of CIRs? If not, what do you think should be included or excluded, providing supporting evidence in each case?

Section 4 is written in a form that assumes that CIRs will be delivered manually in paper form from a known and trusted source. Assuming requests are actually submitted electronically, the process needs to mandate authentication and specify the technology that should be in place to authenticate originating copyright owners or agents – e.g. digital signature.

Inevitably the CIR process adopted and any formats used to submit a CIR will become known and available by anyone on the internet. Without sufficient authentication, it will be relatively simple to send spoof emails purporting to be from copyright owners or agents containing invalid or false infringement information.

Question 4.2: Do you agree with our proposal to use a quality assurance approach to address the accuracy and robustness of evidence gathering? If you believe that an alternative approach would be more appropriate please explain, providing supporting evidence.

Our comments earlier raise significant concerns about the proposals for self-assurance by copyright owners. We do not agree that they are stringent enough to assure the robustness and fairness of the entire DEA regime which rests on them. Internet users may be familiar with many articles and references which examine some of the methods used by some copyright owners and their detection agents and criticisms that have been made and upheld about accuracy, robustness of claims, legitimacy of the operations or the people conducting them.

The French regime (Hadopi) authorises use of specific detection agents. Data protection authorities are involved in checking or authorisation in some EU countries. The commercial sensitivity issues that attach to ISPs' information does not have a counterpart in terms of the copyright owners and their detection activities.

Copyright owners must accept the responsibility for providing correct and validated data in the CIR to identify when the alleged infringement took place, as well as providing sufficient data to enable identification of the alleged infringer. There should be no expectation that the ISP will be required to error check and correct submissions. Any such activity would increase the process burden on the ISP and potentially risk incorrect identification of alleged copyright infringers.

It would amount to an entirely unfair transfer of responsibility and costs from copyright owners and onto ISPs to approach the issue from any other perspective. It is eminently sensible that the incentive to make proper notifications to ISPs rests with copyright owners as far as possible and certainly for matters which are within their control, e.g. to check that inaccurate and incomplete information is not provided to ISPs.

Question 4.3: Do you agree that it is appropriate for Copyright Owners to be required to send CIRs within 10 working days of evidence being gathered? If not, what time period do you believe to be appropriate and why?

The guiding principle which should be adopted to determine "appropriateness" must capture both the following elements

- any time elapsed between detection of alleged infringing P2P file-sharing activity on behalf of the copyright owner and the time that a copyright owner sends a CIR about that incident to an ISP is as short as possible; and provided that
- the copyright owner does not compromise production and provision to an ISP of accurate information (e.g. time stamp) using a robust methodology and an audit trail to enable verification.

Any extended elapsed period will reduce the likelihood of an ISP having relevant data available to make an IP address match which could link a CIR to a subscriber. Shortening this period must not be achieved, however, at the

30 July 2010

expense of reducing the standard on which allegations are based : ISPs, subscribers, regulators and those involved in appeals must have the information they need to implement the DEA fairly, proportionately and in accordance with due process.

On the basis of BT's current understanding, a period of 10 working days from evidence being gathered to a CIR being sent to the ISP seems to be appropriate, given:

- what the DEA envisages; and
- the basis on which copyright owners intend to make their allegations of infringing file-sharing through use of P2P, i.e. the detection methods used will be in real-time such that IP addresses provided in any allegation in a CIR will correspond only to incidents detected in real-time.

It would be inappropriate to require an ISP to process any CIR in which more than 20 days have elapsed between the date the alleged infringement occurred and the time the CIR is provided to the ISP.

The tight timescales of Ofcom's current proposals for CIR notification and escalation makes it even more crucial that cut-off times for submission of CIRs and their processing are clear.

Ofcom must ensure that the Code enables these periods to be reviewed and revised in the light of issues emerging during practical implementation. The whole issues of timelines for CIR and notifications will have to be revised entirely if the IP addresses captured on behalf of a copyright owner are decoupled from infringement allegations made in a CIR.

Question 5.1: Do you agree with our proposals for the treatment of invalid CIRs? If you favour an alternative approach, please provide supporting arguments.

BT cannot guarantee linkage of an IP address to a particular subscriber and it cannot provide evidence that an infringement has taken place by making such a linkage.

There are multiple ways in which a subscriber could be misidentified and therefore lead to an invalid notification being sent to an ISP by a copyright owner. This means that qualification should always be made to the confidence that can be placed in identification of a subscriber being correct on each and every occasion using the methods that copyright owners are likely to deploy. Similar qualifications should also be made in a copyright owner's subsequent use of and reliance on any information that has been logged by the detection methods employed by it, e.g. in the course of an appeal.

In addition to the situations described in section 5.3 of the Consultation the following common situations which are industry- wide and affect many internet subscribers and users and can give rise to unreliable identification include

30 July 2010

- where an ISP's systems are reliant upon customer input data to identify the end user e.g. Pay-as-you-go services rely upon the customer details given to register an account. Such details can be and often are bogus.
- Compromised customer computers or home routers could be used by a third party to download illicit material without the knowledge of the customer. This could occur with either physical access to the computer or through malware.
- Spoofed IP addresses. The practice of sending IP packets with forged source IP addresses.

It is common industry practice for ISPs to use Universal Data Protocol (UDP) to collect logging data. This means that the data is only transmitted and collected on a best-efforts basis. Data collection is, therefore, not guaranteed. This could result in there being no logging records in the ISPs systems to confirm or contradict a CIR.

The different characteristics of the various BT internet product types will mean that for each one there will be a set of circumstances relating to it under which misidentification could occur.

There is no logic in requiring ISPs to act on invalid CIRs, in particular those that are classed as invalid for the reasons identified in section 5 of the Consultation.

We do not think there is any reason to require a standard set of rejection Codes as part of the Code, certainly not as a priority compared to other fundamental issues. It may be useful, though, for ISPs to provide information on a longer timescale about the common reasons for non-matches at the ISP end.

There is no reason, however, to prescribe a 10 day turn-around time for notification back to copyright owners.

We are concerned, again, that the approach seems to push requirements onto ISPs to create systems and data to enable maximisation of notification volumes. We find it hard to discern why the factual matters in paragraph 5.3 which may result in a no-match or an unreliable match are matters pertinent to a 10 day turn-around for copyright owners or why systems should be built to accommodate such a requirement.

An ISP's costs for processing a notification - even if it turns out to be invalid - must be covered in any event.

Question 5.2: Do you agree with our proposal to use a quality assurance approach to address the accuracy and robustness of subscriber identification? If not, please give reasons. If you believe that an alternative approach would be more appropriate please explain, providing supporting evidence.

30 July 2010

A general observation is that BT doesn't have one process for subscriber identification across its broadband product portfolio. Instead BT would have a different process for each different internet product. This would mean separate validation of the process for each of the products within the scope of the DEA.

BT has concerns about handling and exposure of information on the nature of its systems and processes, since this is highly sensitive and commercial information about its core business operations. Any compromise of systems or processes caused by the documenting and sharing of this information would potentially put at risk customer service, generate the opportunity for customer data confidentiality violations, as well as causing possible damage to BT brand and image.

In previous responses to BIS we have made clear that in any event it would be completely unacceptable for copyright owners to have access to such information.

We are happy to work with Ofcom on how to resolve this issue so that it can be dealt with in a way that can provide a suitable assurance of quality without compromising confidentiality and commercial sensitivities.

Question 5.3: Do you agree with our proposals for the notification process? If not, please give reasons. If you favour an alternative approach, please provide supporting arguments.

The DEA provides the option for the notifications to be sent by email or post. As a business, BT increasingly relies on electronic methods of information delivery (e.g. online billing) and our preference would be to send notifications via email as we did in the P2P MoU in 2008/9. We therefore welcome that the Code allows either method for 1st and 2nd notifications. Email also provides the ability to provide dynamic links to information which might be helpful and useful in a way that is not feasible in a physical letter.

The notification process indicated in paragraph 5.11 does not seem to be more proportionate or objectively justifiable than the other two options in any respect. It is very rigid and far fewer CIRs would be required to trigger notification and escalation against a subscriber compared with the method envisaged by BIS. Basing the process on just three CIRs received in three successive months does not amount to an approach that deals with "behaviour over time" as asserted and it is not fair or proportionate. The elimination of all factors that could provide some proxy for taking account of seriousness and level of seemingly persistent infringing activity is not an improvement. As BT has indicated in earlier comments, the way that copyright owners currently choose to detect suspected infringing activity includes intrinsic value assessments. Ofcom should develop an approach that factors that in to improve the proportionality and objective justification for the notification process.

30 July 2010

Based on our experience under the P2P MoU and our reservations and concerns about many aspects of Ofcom's proposed approach to timings for the processing of CIR and the treatment of CIR that might be invalid for a variety of reasons, the compressed and extremely rigid timetable is unrealistic. Further, Ofcom has not made any attempt to deal with the interaction of the process with subscriber appeals.

We do not believe a one month period between the first notification being sent to a subscriber, and the possibility of a second CIR being issued with a subsequent notification is sufficient. This also applies between the 2nd and 3rd notifications. The current timeframe within the document allows 10 days for a rights holder to send a CIR, and another 10 days for an ISP to have the opportunity to reject a CIR. Assuming after 20 days, a notification is sent, this gives a very small window for mail delivery, the subscriber to receive, open and understand the notification, and then have the opportunity to change behaviours, or take action to identify the source of the alleged infringement. Potentially, further alleged infringements could occur before possible corrective actions could reasonably be taken.

We believe the notification process should be suspended for an individual pending resolution of any subscriber appeals. Given an alleged infringement is being challenged, it will cause considerable confusion and data complexity to be working on an assumption of guilt of a previous notification, whilst an appeal is being made. The type of notification letter sent and the actions taken subsequently will be different depending on the result of an appeal. At best this would cause rework and revisiting previous notifications with cost implications.

Insofar as the process proposed would form the basis for potential technical measures it is unfair and disproportionate in its harshness. Its only merit appears to be rigid simplicity in terms of describing the process.

Ofcom could and should revise its proposed approach significantly.

For any notification process that is adopted, the obligation must fall on a copyright owner to ensure that CIRs are only raised in accordance with the timeframe articulated by any Code, e.g. such as proposed in paragraph 5.11 of the Consultation. A copyright owner would therefore need to ensure that:

- multiple CIRs are not generated against the same alleged infringement
- a CIR is not raised against any infringement alleged to have occurred prior to one that previously resulted in a notification being sent;
- a CIR is not raised against any infringement alleged to have occurred within the elapsed periods of time allowed for in paragraph 5.11 since the first or second notification occurred.

We would wish to receive clarification directly from the ICO about the proposals made in paragraph 5.18 of the Consultation

Question 5.4: Do you believe we should add any additional requirements into the draft Code for the content of the notifications? If so, can you provide evidence as to the benefits of adding those proposed additional requirements? Do you have any comments on the draft illustrative notification (cover letters and information sheet) in Annex 6?

We believe that it may be helpful for subscribers if the wording and form of the relevant “statutory” elements of the notifications can be agreed between ISPs so that they use a standard approach. We would be happy to engage in further dialogue with industry to achieve that. Beyond this, we consider that there should be no barrier to ISPs sending the “statutory” content together with independent material that might be helpful and useful to our customers, e.g. to point people to relevant material available from the IPO or from www.getsafeonline.org as part of the information sent to the subscriber.

Question 6.1: Do you agree with the threshold we are proposing? Do you agree with the frequency with which Copyright Owners may make requests? If not, please provide reasons. If you favour an alternative approach, please provide supporting evidence for that approach.

Paragraph 6.5 is ambiguous in relation to the contents of a given Copyright Infringement List and whether it should be possible to correlate “anonymised” subscribers across different lists. It raises a number of queries, inconsistencies and concerns about the role of third parties and sharing of information across copyright owners via disclosures made to third parties and practical system design and security issues.

Should the unique anonymous identifier assigned by an ISP for a given subscriber be:

- the same reference for all copyright owners?
- different references for different copyright owners?
- different references for different third parties agents (i.e. if a single copyright owner has multiple agents?)

We are concerned by the implications of a single “anonymised” consumer reference cross all copyright owners. It provides the opportunity for a third party who acts for more than one copyright owner being able to correlate lists, and use this information to identify repeating “infringers” for more than one copyright owner. We are not clear that the DEA envisaged this.

Should CILs be correlated against the copyright owners or the third parties agent, i.e. if the third party agent represents more than one copyright owner, would their CIL contain data relating to all of the copyright owners they represent? Alternatively, if more than one third party agent is used by a given copyright owner, should an infringement list for the agent only relate to the specific CIRs they submitted.

Careful consideration needs to be given to the role of any third parties involved and their relationship and roles vis a vis a copyright owner needs to

30 July 2010

be transparent and clarified for ISPs, and others. We believe Ofcom should take measures to ensure the bona fides and good practice of any third party detection agent, Licensing them appropriately should be considered as it is in other countries. The sharing of information about internet users communications and their content (even in a so-called “anonymised” form) raises concerns about compliance with other regulations and laws that BT is subject to ,e.g. under data protection or competition (information –sharing) laws. Confirmation should be given that all third party agents will be suitably validated, and that if the Code does enable third parties to receive data from BT that BT would not be contravening any data protection legislation by providing data to them.

BT does not believe it will be possible to support copyright infringement lists with a manual process. Any process would be highly manpower intensive and carry a high probability of errors. The result would be incorrect data being provided on infringement lists

We do not know what Ofcom currently envisages as the starting point for Code obligations relating to the compilation and provision of CIL and whether Ofcom is making an assumption that “soft launch” of the Code could take place with manual processes.

On the basis of BT’s evaluation, either CIL requirements would need to follow in later phase of implementation of the Code, as a phase 2, or soft launch would need to be deferred to a time that would enable CIL systems to be developed.

It would be unreasonable for the turn–around time for a CIL report from an ISP to a copyright owner to be as short as 5 days as proposed in paragraph 6.7. ISPs will have to build completely new systems to deal with CIL and we do not know if we will obtain the clarity we seek on the queries above so as to enable us to design and implement non-complex systems from which information can be retrieved efficiently and in compliance with confidentiality, competition (information sharing) and data protection requirements.

The Code should provide for no less than 10 working days for responding to a proper request for a CIL.

Question 7.1: Do you agree with Ofcom’s approach to subscriber appeals in the Code? If not, please provide reasons. If you would like to propose an alternative approach, please provide supporting evidence on the benefits of that approach.

“Subscriber Appeals” are adjudications not appeals

Section 7 of the Code, reflecting the language used in the DEA, purports to set up a process for subscriber ‘appeals’. Regardless of nomenclature used, the reality of the situation is that the process is not, in the usual sense of the word, an appeal. Rather, where the subscriber and the Qualifying ISP or

30 July 2010

Qualifying Copyright Owner do not agree on the facts, it represents the first independent adjudication of the disputed issue.

For there to be an appeal, there has to be an initial decision which can be appealed. That is not the case here. Instead, we just have allegations made by one party against another (i.e. allegations of copyright owners against subscribers) which have not yet been tested in a way which results in an independent finding of copyright infringement.

The burden of proof should be on copyright owners not subscribers

The true nature of the proceedings is relevant in relation to the burden of proof. The effect of characterising the first independent hearing of the disputed issue as an “appeal” rather than as an “adjudication” is to inappropriately legitimise the notion that it is acceptable to take the evidence provided by copyright owners at face value and require the subscriber to provide a case, including evidence, to clear their name. Given the relative position of the parties, and the potential interference with a person’s rights that could occur in such circumstances, we consider that it is unreasonable to shift the normal burden of proof in this way. We do not think that it is fair or equitable for the starting point of this appeal/adjudication process to be that copyright owners do not have to substantiate and prove their case.

Indeed, we note that the whole Notifications process set out in the Act, and now potentially to be implemented by means of the Code, from first through to third Notification letter, and subsequent adoption of a subscriber onto a Copyright Infringement List, is based simply on the assertions of copyright owners. The consequences for subscribers, if these assertions remain unchallenged, could ultimately cause significant detriment to the subscribers concerned. Independent arbitration is needed to provide a crucial check and balance in the process. We contend that for this check to operate fairly and effectively, the starting point should be for copyright owners to have to prove that their assertions are correct, rather than for subscribers to prove that they are incorrect.

Need for genuine rights of appeal from the independent adjudication called “Subscriber Appeal”

The Code provides for an independent body (the “Appeals Body”) which will have the job of determining, among other things, complex areas of copyright law, which would normally, and have been to date, dealt with by specialist courts. The Code neither lays down any requirement regarding the experience or specialisation of the individuals to be appointed to the Appeals Body, or the criteria to be met regarding their independence. Nor does the Code allow for any further appeal into the normal judicial process in cases of disagreement over complex areas of copyright law which could arise in the Appeals Body’s remit. These are matters for the courts and should remain so.

Furthermore, we consider it incompatible with general principles, in relation for example, to Tribunals, that there should be only the one decision maker

30 July 2010

whose decision cannot be appealed. We note that in relation to many other types of Tribunals, there are rights of appeal to a higher body.

We invite Ofcom to consider how the scheme could be rescoped in order to provide an appeal against a first instance decision, and a mechanism for complex issues of copyright law to be resolved, whether by reference to the courts or otherwise.

The Copyright, Designs and Patents Act 1988 section 16(2) provides that copyright infringement to have taken place either by the individuals themselves or by a third party clearly authorised by them to do so. However, the DEA allows for a finding of copyright infringement to be made by the Appeals Body in circumstances where the subscriber has failed to take steps to prevent third parties from using their internet connection, even though they may be totally unaware that their connection has been used for copyright infringement purposes. Clearly they cannot have been said to 'authorise' the alleged infringement in these circumstances, thus the DEA can be said to introduce a different standard of knowledge and intent to that which would be required by the courts.

Access to the "subscriber appeals" process should be affordable by all

The draft Code anticipates that fees may be charged to subscribers wanting to challenge allegations made about them. We understand that the intention behind this is to discourage potential "timewasters". Whilst we agree that abuse of any legal system is inappropriate, it does tend to be rare. Measures to prevent timewasters should not inadvertently penalise the vast majority of subscribers whose appeals are genuine and who are seeking to clear their names because, for example, their networks have been used without their knowledge or permission. Access to justice must remain affordable to all, and if any fees are to be imposed these should not be such as to deter genuine appeals by any individuals in society. Indeed, we consider that for at least a first appeal, there should be no fee – with fees only being imposed on subscribers who have previously made repeated failed appeals.

Concerns with the operation of the scheme, in practice

We suspect that a substantial proportion of alleged copyright infringement takes place in the family home, or other shared premises, in circumstances where the subscriber (often a parent), has little if no idea, or their household's (children, teenagers, young adults, friends, carers) activities online. We very much doubt that they would be prepared to disclose to copyright holders, or the ISPs, that their children are the likely culprits, or that they would be willing to restrict their children's access to the internet which is used extensively for educational purposes, social networking and all other legitimate activities conducted online. We therefore believe this is likely to result in large numbers of entirely innocent subscribers being pursued by copyright owners for copyright infringement.

30 July 2010

The Code provides for a robust and accurate process to be put in place to record IP addresses and match them to particular subscribers. In this case it is difficult to see how ISPs' records could be challenged by subscribers, as there would not be an alternative data set which could be used to provide alternative information. Further, the relevant information may not have been retained and thus may not be available in the timescales in which an appeal could be brought. It is also highly unlikely that a subscriber would have kept a note of their IP address, bearing in mind most of the time these will be dynamically assigned, every time they go on line, or should be expected to do so (unless of course the intention is that every subscriber should anticipate receiving a notification of copyright infringement every time any online activity happens and prepare for that eventuality in this way). For these reasons, again, we contend that it is right for there to be an appropriate, independent and rigorous check on the assertions made by copyright owners.

Overall, we consider that little thought, if any, has been given to the practical aspects of how a subscriber could bring an appeal. It is clear from the way that dynamic IP addresses are allocated that linking one to an individual subscriber at a specific time is not an exact science. The records provided by an ISP should be accepted on an 'as is' basis by the Appeals Body, with no potential for liability on the part of an ISP if the records are challenged by a subscriber. The focus of the Appeals Body should be on the way evidence is collected and provided by the copyright owners is gathered, given they are making the allegations in the first place. Further, it is disproportionate for the Appeals Body to be able to make a finding of liability by ISPs to subscribers in these circumstances.

The draft Code fails to deal with the effect of an appeal on the operation of the Code

The Code does not provide clarity on the effect of making an appeal on subsequent notifications which may be received by the subscriber concerned. For example, if the subscriber chose to appeal the second notification, this must have the effect of 'staying' the notifications process. Otherwise a subscriber could receive a third notification whilst their case was outstanding, be placed on the Copyright Infringement List, their identity disclosed, and then win their appeal. In those circumstances the second notification would be rejected and their personal data would potentially have been inappropriately disclosed and without legal sanction. This places ISPs at risk of allegations of breaching data protection legislation

Conclusions

In summary, the whole notifications process, ending with the Appeals Body, starts from an assumption that what the copyright owners say is a true statement of what has happened. The onus is placed on subscribers concerned to take action and incur costs in order to clear their names. Such a regime does not balance equally the interests of copyright owners and subscribers. It is therefore essential that there are appropriate checks and balances in the system. The appeal/adjudication process should put the onus

30 July 2010

on the copyright owner to prove its case. Even if that happens, we remain concerned that it is difficult to see how a subscriber could realistically challenge an allegation of copyright (one of the grounds for appeal) without access to specialist legal advice. There should be access to justice (including, if necessary, access to legal advice) at a price which is affordable by all. Finally, the Code does not, but should, provide for further appeal, to the courts or otherwise, should a subscriber wish to challenge a decision of the Appeals Body that a copyright infringement had taken place.

Question 8.1: Do you agree with Ofcom's approach to administration, enforcement, dispute resolution and information gathering in the Code? If not, please provide reasons. If you favour an alternative approach, please provide supporting evidence on the benefits of that approach.

The DEA is a completely new and unusual piece of law and regulation, for which there is no precedent in the CA. The lack of clarity and certainty on virtually every aspect of its interpretation and application is immense. It would be thoroughly unreasonable for Ofcom to invoke requirements in these areas against providers of communications providers/ISPs as though they are simply a seamless update of developed areas of the CA.

We are also unclear on what can or should be expected in terms of disputes and dispute resolution between ISPs and copyright owners, demand and expectations of appeal bodies and the information that may properly be demanded of BT by anyone else. The power of appeal bodies to require information and potential enforcement is broad

We are clear as the House of Lords Delegated Powers & Regulatory Reform Committee was in its Second Report on the Digital Economy Bill that even though the DEA has been introduced into the existing CA, the fit and analogy with other matters that are already regulated under the CA does not go all the way.

It would be utterly unreasonable for Ofcom to approach this new area as though it was an area of regulation that has developed over many years, where culpability of communications providers can be assumed (they are not engaged in copyright infringement by providing internet access services) and that it will be proportionate and fair to enforce against them at heavy and strict levels from the outset and for any kinds of failures and omissions.

In our previous responses to BIS, BT asked for

- clarity that enforcement would not be used as a proxy for landing ISPs with financial liabilities akin to the losses that copyright owners assert are attributable to infringement;
- sought clarification of the approach that would be adopted for system and process problems such as systems not coming into place on anticipated dates, falling over, etc;

30 July 2010

- sought assurance that it would have the autonomy and flexibility to prioritise dealing with demands from law enforcement authorities without facing enforcement action for meeting notification targets.

Ofcom's guidance and principles should address and provide reassurance on these points.

We anticipate that an ISP will regularly be placed in the difficult position of attracting exposure to claims and criticism, for example on privacy and fairness grounds, when trying to fulfil DEA obligations. In order to manage such competing risks, an ISP will need Ofcom to provide principles, guidance and clarity about the enforcement approach it intends to adopt. Ofcom should take specific account of the existence of such competing risks in developing its enforcement approach to ensure that what it adopts is fair and proportionate.

Ends

Annex 1 Detailed Comments on Wi-Fi and Mobile Broadband

1. Wi-Fi and mobile broadband access have many similarities of relevance to the application of the initial obligations code

In paragraphs 3.11 and 3.12 of the Consultation, Ofcom has proposed that mobile ISPs should not be subject to the Code for the following reasons:

- Mobile networks are less conducive to online copyright infringement due to speed and capacity constraints, traffic management policies and pricing. Copyright owners claim that more than 95% of alleged incidents were on fixed networks;
- Mobile networks assign public IP addresses differently to most fixed ISPs, typically having more limited allocations of IP addresses. An IP address assigned to a mobile ISP could be used by a number of individual subscribers at the time of an alleged copyright infringement.

However, in paragraph 3.22 Ofcom says that it regards Wi-Fi as offering a fixed service on the basis that Wi-Fi is offered from fixed locations and is not a licensed mobile network., Thus BT Openzone, by virtue of being part of BT's wider internet service provision, would be brought within scope of the Code.

We question whether the assessment of mobiles is based on clear evidence – we have not seen the evidence on which it is based - but since these factors are considered relevant in making this assessment, Ofcom do not appear to have considered any of the technical and practical similarities which exist between the services provided by Wi-Fi and 3G broadband, including those specific points stated by Ofcom as forming its rationale for excluding mobile internet access from the scope of the initial obligations. Ofcom has not applied these reasons to Wi-Fi, nor has it applied its own stated criteria of objective justification, non-discrimination, proportionality and transparency, in making this decision. Ofcom has not followed the Government's requirement that the initial obligations should not fall on ISPs where there is a low level of infringement.

It is discriminatory, disproportionate and not objectively justifiable to treat public Wi-Fi as fixed internet service provision and thus cause BT's public Wi-Fi business to be brought within the scope of the Code. Public Wi-Fi should be treated the same way as mobile internet access provision because:

- the technology used to provide it works in a similar way to mobile technology;
- It shares the same issues as mobile would in terms of compliance with the Code;
- BT's Public Wi-Fi customers should not be counted as within scope in the same way that O2 and Orange mobile customers are not included.

The inclusion of Wi-Fi broadband would directly discriminate against BT since it would be the only public Wi-Fi business in scope of the Code, since BT is the only named internet access provider operating a Public Wi-Fi network.

30 July 2010

Organisations looking to establish a public Wi-Fi service may be less willing to purchase the service from BT because of the additional compliance costs and uncertainty they would face compared to taking service from other Wi-Fi providers.

In all relevant and meaningful respects, Wi-Fi is analogous to 3G broadband and both should be treated the same for the purposes of the application of the Code for the following reasons.

Mobile and Wi-Fi signals are both 'fixed'

In the same sense that Wi-Fi is said by Ofcom to be offered from a fixed point, mobile is also offered from a fixed location i.e. the location of the mobile mast, which is equivalent to the Wi-Fi hub. The only difference between the two being the mobile mast signal strength and resulting coverage area. The mobile mast signal is much stronger than the Wi-Fi hub signal strength as it is designed to cover a greater distance and provide service to a greater number of users. The Wi-Fi signal is radiated from a single radio access point for a particular Wi-Fi coverage area the same way as GSM and 3G radiate from a mast for a mobile coverage cell. Neither service offers complete blanket coverage, as both are restricted to the coverage provided by the signal from the central point i.e. the mast or hub. The fact that Wi-Fi is not licensed as a mobile operator is irrelevant to the analysis of whether it is a fixed internet access service or not. For completeness, the Wireless Cities are provided by means of public radio access points, but on a scale which makes the service even more comparable to a mobile cell because of the wider range of coverage achieved.

The amount of P2P traffic is likely to be very similar

The level of P2P traffic on Wi-Fi networks is likely to be very similar to the level on mobile networks, as speed and capacity constraints are comparable. Both consumer and business Wi-Fi networks provided by Openzone in the UK are subject to a maximum bandwidth allocation of 500 kb/s per hub which is a contended service. The capacity of services into premises such as hotels and coffee shops may vary depending on whether they are served by fibre or ADSL technology, but ultimately all are contended services which limit the speeds available to individual users. Further, as the majority of locations with higher capacity are hotels and Wi-Fi internet access is provided predominantly to support business conferences, the incidence of file sharing in these circumstances is likely to be low given the nature of the end users.

Wi-Fi and mobile devices are increasingly similar

The majority of Wi-Fi use in public places is through smart phones and other mobile devices. The majority of file sharing applications are written for use with PCs running on Windows operating systems. The nature of p2p requires a file sharer to make uploads as well as downloads, and uploading on Wi-Fi is a more complicated and less convenient process than on traditional fixed

30 July 2010

networks. It is also subject to interruptions due to the automatic break after 30 minutes using a particular IP address.

IP allocation technologies are the same

Wi-Fi networks allocate IP addresses to users in a similar way to mobile networks using DHCP (Dynamic Host Configuration Protocol) which allows use of a public IP address for periods of up to 30 minutes maximum. These IP addresses are regularly re-used by customers. However, there is limited availability for exclusive use of an IP address during a session due to restricted capacity. During busy periods (which are increasing as Wi-Fi use grows), it is necessary to share single IP public addresses. This can involve up to 65,000 users per public IP address. In this case it is not possible to identify the user of a particular session at a particular time just from the IP address, it is also necessary to know the port number as well. This can be achieved using PAT technology, but the costs of the size of capacity required to store both IP addresses and port numbers, which could involve up to 65,000 per public IP address at any one time, would be disproportionately high and would impact on the viability of the Openzone business model.

Identifying an individual user from an IP address is similarly difficult

The vast majority of BT Wi-Fi use is on electronic vouchers purchased from the BT Openzone and BT Fon website and hotspot, and access can also be paid for via paper vouchers sold primarily through hotels, coffee shops or other business outlets. The majority of use paid for by these methods is anonymous except in the sense that any purchased using a credit card could theoretically be traced back through the credit card provider. However, this would be a disproportionate requirement and fraught with data protection/customer confidentiality issues. The majority of voucher use is for a one-off sessions, and about one third of this use is from overseas customers visiting the UK., Disproportionate effort and cost would be required to find out who has bought a voucher at any one time – all vendors and purchasers would need to be logged and those logs made available to service providers. This disproportionate requirement would severely impact the pay- as-you-go voucher business model as well as requiring significant additional tracking and recording on electronic voucher access. Furthermore, there is no guarantee that user details collected at the time of sale would be accurate. A user is entitled to decide on the details he provides and if any user intended to use the network to unlawfully file share, it is highly likely that they would not give their correct name and address or e-mail address details.

Counting Wi-Fi users as separate broadband subscribers is not appropriate

The BT Total Broadband package for fixed internet access also includes free public W-Fi access for use when subscribers are away from base. However, these are subscribers for the purpose of determining the size of the fixed internet subscriber base, and should not be double counted for the purpose of the wireless broadband subscriber base as this gives a distorted view of the overall subscriber base. This Wi-Fi facility is just another means available for them to access the internet having paid for a subscription to the fixed service.

As these customers have fixed broadband, if they were to engage in file-sharing, they would be far more likely to do so on their fixed access link due to the capacity and other disadvantages of attempting to do using Wi-Fi. The fixed networks are of course not provided on the “pause”, in other words, at limited session time per IP address and port allocated in the way that public Wi-Fi is provided. This is another reason which limits its effectiveness as a route to file sharing.

2. Ofcom proposals on churn and Wi-Fi

Paragraph 3.17 of the Consultation proposes that Ofcom would review the qualification criteria in the Code taking into account the number of subscribers and the volume of potential copyright infringement reports. It is not possible to ascertain with any certainty the number of Wi-Fi subscribers which BT Openzone and BT Fon has at any one time. The majority of use is via vouchers. Customers can buy any number of vouchers for one-off use and BT Openzone would not know how many a particular user had bought in any period, e.g. during the course of the year, or if they had passed any vouchers to third parties. The number of Wi-Fi subscribers at any one time would be very difficult (impossible) to quantify at any given time.

Paragraph 3.28 refers to pay-as-you-go mobile broadband operators which could fall to be subject to the Code needing to ensure that they collect information about their subscribers. For Wi-Fi users, this would require details of each user for every single voucher used to be collected at the point-of sale, or registration details of every ‘free use’ made to comply with this aspect. The costs of collecting this information, and storing it would be disproportionate to the level of benefit gained, particularly as the data would be likely to be little better than worthless.

Paragraph 5.3 recognises a variety of circumstances in which an ISP will not be able to identify a subscriber. These include that the ISP does not hold an address for the subscriber and it is not reasonably practicable for the ISP to obtain it. As indicated, this situation is overwhelmingly likely to be the case for Wi-Fi. On what basis can Ofcom conclude otherwise? Paragraph 3.31 – Ofcom on steps to be taken to protect networks from third party use. Future developments by hardware providers will further reduce the visibility of the Wi-Fi operators as to who their customers are. Evolving standards being developed are not under the Wi-Fi operators direct control.

3. Further comments on Ofcom’s views on definitions and the impact on Wi-Fi

In paragraph 3.22, Ofcom state that any agreement, express or implied, with a subscriber is sufficient to bring the service in scope of the Code under the definition in the DEA of ‘subscriber’.

However, in paragraph 3.30 Ofcom say that where there is no such apparent agreement, the person making open access available would be considered to

30 July 2010

be a subscriber for the purposes of the Code. However, the DEA does not legislate that different application of the Code in these different circumstances is predicated on whether payment is required or not by a party making services available.

In cases where Wi-Fi is provided in conjunction with other goods or services, such as in a coffee shop or hotel, the definitional issue is not addressed as Ofcom simply say that as such providers would fall under the proposed 400,000 subscriber threshold they will not be subject to the Code.

However, Ofcom goes on to say that when reviewing the Code they will consider these factors when considering whether this form of internet access provision should be within scope of the Code –

- Consumer prejudice
- Level of copyright infringement in such networks
- Costs to operators

These are clearly relevant factors which should be considered in all cases when deciding whether or not a particular form of internet service provision, or business model should be within scope of the Code.

The vast majority of W-Fi use is voucher based, most of which are used once, and a third of which are for use by people visiting the UK. In the case of hotels, the majority of business is in London and used primarily by foreign nationals. To suggest in paragraph 3.28 that such providers should collect information about who their subscribers are so as to comply with the Code is a disproportionate requirement and in any case of little use given the use of these services by foreign nationals. In the case of a user intending to file share, what incentive would they have to give accurate information and how could it be verified? Is it really the case that users would be required to show their passports to verify their identity before being allowed to buy a voucher to access the internet?

It is also difficult to characterise a hotel or coffee shop as an ISP when internet access is sold along with other goods and services. To argue that hotels and coffee shops are within scope of the definition of an ISP by selling access vouchers along with other services is not an argument which can be objectively justified.

Ends