Cover sheet

BASIC DETAILS

Consultation title:	Online Infringement of Copyright and the Digital Economy Act 2010
To (Ofcom contact):	Campbell Cowie
Name of respondent:	Jim Killock
Representing (self or organisation/s):	Open Rights Group
Address (if not received by email):	

CONFIDENTIALITY

Please tick below what part of your response you consider is confidential, giving your reasons why

Nothing

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)? NA

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Jim Killock Signed (if hard copy)

About the Open Rights Group

The Open Rights Group is a grassroots digital rights advocacy group based in the UK. It aims to increase awareness of digital rights issues, help foster grassroots activity and preserve civil liberties in the digital age. It is funded by donations rom over 1,400 individuals and small grants, and has an active community of 16,000 supporters.

Detail of Respondents

Prepared by:	Jim Killock
Responding on behalf of:	The Open Rights Group
Date:	30 July 2010
Address:	Open Rights Group Langdale House, 11 Marshalsea Road, London SE1 1EN United Kingdom
Telephone:	+44 (0)20 7096 1079
Email:	info@openrightsgroup.org
Website:	http://www.openrightsgroup.org

Contents

1 Introduction

ORG believes another round of consultation is essential to meet Ofcom's obligation to properly consult on these proposals. Large parts of the IOC's requirements under the Digital Economy Act (DEA) are missing from the draft, and others are entirely or largely faulty. We are not consulting on a legitimate option that Parliament could in good faith adopt as a Statutory Instrument: and as a result we are being denied the opportunity to comment on some of the most important aspects of the code.

In our response, we outline the key problems we have identified with the Code, which demand another round of consultation. The most serious of these relate to the requirements for standards of evidence, both for copyright owners and ISPs, which are missing from the code. These are requirements under the DEA. Also seriously flawed are the requirements for appeals processes, missing requirements for letters to subscribers, privacy implications of the arrangements and definitions of ISPs and subscribers.

We then move to some potential problems that are left in the code. These too are substantial, and carry significant risks, particularly to small businesses, community groups and open wifi networks, and most importantly, their users. Open wifi is a common good, not a problem to be discouraged. It provides zero-cost access to information to users, and contributes to a widespread culture of access to communications, benefiting society, culture and the economy. Discouragement of open wifi - which is likely to be the result of this code - is simply a bad idea, and a disproportionate cost against the possible costs of copyight infringement.

Finally, we suggest a number of problems with the whole process, including the lack of an economic impact assessment, and privacy impact assessment, and the means by which Ofcom can try to rectify these. We recognise that Ofcom has a legal duty to carry out the requirements and put forward a process to govern the letter writing programme, as well as report on its progress and levels of "online copyright infringement". However, Ofcom also has a duty to protect both competition and promote 'consumer interest'. In relation to these wider goals, we take this opportunity to comment on the means by which Ofcom can do justice to its wider remit in relation to these obligatons.

2 Why we need another round of consultation: severe errors and omissions in the consultation document

The code itself as consulted on does not in large substance comply with the DEA or the Communications Act more generally. This is itself enough reason to reconsult on a compliant code. We detail the non-compliance in this section.

2.1 No definition of the process by which evidence is collected

The Digital Economy Act's sections 3-16 are supposedly designed to tackle downloading via 'peer-to-peer' networks, although none of this is discussed or defined in the Act. Instead, the Act and the code talk of 'online copyright infringement', covering an incredibly wide range of behaviours, which may be detected, reliably or unreliably by a huge variety of means. This dangerously wide definition and potential for less than robust or inappropriate detection procedures is balanced by a requirement to narrowly define the method by which infringement is identified. Unfortunately this is missing from the code, leaving us unable to evaluate what infringement is supposedly detected and whether the methods may be robust.

Section 7/124E(2) of the DEA requires that the initial obligations code makes the required provision about Copyright Infringement Reports (CIR) by specifying "requirements as to the means of obtaining evidence of infringement of copyright for inclusion in a report", and "the standard of evidence that must be included". The draft initial obligations code makes no provisions specifying the means of obtaining evidence of infringement of copyright for inclusion, and neither does it make provisions specifying the standard of evidence that must be included.

Section 3.5 to 3.7 of the draft initial obligations code outlines, in relation to evidence gathering process what it calls a "quality assurance process". But this process does not specify the means of obtaining evidence or the standard of evidence included, only that the copyright owner will have to follow the process outline in their QA

report which is to be submitted to Ofcom. The DEA does not require such a QA system.

The previous Government clearly intended for the initial obligations code to provide details defining how the evidence will be collected by copyright owners and the standard of evidence as a way of guarding against the likes of ACS:Law using the DEA notification process. The initial obligations code was meant to establish clear criteria and processes as a way of guarding against subscribers being accused of copyright infringement in error. Lord Young amongst others stated that:

> Clearly, it will be important that the appeals body set up by the code should be capable of determining whether a copyright infringement notice has been properly generated, so it will require some technical knowledge and expertise of, for example-I stress the importance of this-whether an infringement has occurred; whether the time and date stamp is accurate; whether the IP address was correctly captured and recorded; whether it has been properly handled by the ISP; and whether the subscriber has been properly identified from the IP address and the time and date stamp provided. As I have said on a number of occasions, that means an audit trail, a validated evidence base, not incomplete information. No system is infallible, but we are talking about serious evidence that can be technically validated and proved and that has to be chronologically correct. [1]

The standard of evidence and the way it is processed is of utmost importance. If the means of obtaining evidence and the standard of evidence on which copyright infringement reports are based is not robust, potentially thousands of subscribers will be sued by copyright owners even though no credible evidence has been established. CIRs will be the basis for those subscribers being put on a "copyright infringers list", i.e become relevant subscribers for the purpose of technical measures which may be introduced at a later date. The more immediate consequence for subscribers who have been put on the copyright infringement list is that copyright owners will take them to court for copyright infringement, on the basis that they are assumed to be "repeat infringers".

It is apparent from Lord Young's comments in Parliament that the Government intended the initial obligations code to make detailed provisions about the way in which evidence is gathered by copyright owners and later processed by ISPs, so that any mistakes can be treated as non-compliance with the initial obligations code, which is to be enforced by Ofcom.

> Proposed new Section 124E(5) in Clause 8 and proposed new Section 124J(4) in Clause 13 allow the code to make provision for financial penalties when an ISP or a copyright owner fails to comply with one of the obligations or the provisions under the codes that put those provisions into practice. It might help if I explain the Government's thinking. Failure on the part of either a copyright owner or an internet service provider to comply with the obligations or the code could have a damaging effect on a subscriber, a copyright owner or an ISP. In that situation it is appropriate that there should be some deterrent to ensure that the obligations and the code are complied with. We have suggested two different types of deterrent, because the harm could occur in different ways, as the noble Lord, Lord Howard, identified. For example, if an ISP fails properly to process the copyright infringement notices, the notifications will not be issued and the resultant anticipated impact on the subscriber's infringement will not materialise. This is a generic failure causing generic rather than specific harm and, because it is generic, is appropriately dealt with through a fine. However, if a copyright owner makes a mistake in transcribing the time and date of an alleged infringement, an ISP might issue a notification to the wrong subscriber. If technical measures are in place, an ISP might even impose a technical measure on the wrong subscriber. This could cause real financial or other harm to the subscriber, who might then choose to take action against the ISP in relation to any loss suffered. If the subscriber were to win damages from the ISP in these circumstances, it seems only reasonable that the copyright owner responsible for the error should indemnify the ISP for any loss or damage resulting from the error. We have put these two different mechanisms into the Bill not as alternatives but as complementary tools, because different types of harm could be suffered dependent on where the error or omission occurred. That is not to say that both would be used in any individual case, but the code should be able to contain both and apply them as appropriate. I hope that that has clarified the matter for the noble Lord.[2]

The Government also clearly recognised that subscribers need to be protected against negligence by copyright owners and internet service providers in processing the evidence relating to a copyright infringement report, and

1 http://www.theyworkforyou.com/lords/?id=2010-01-20a.1009.3&s=evidence+speaker%3A13450#g1026.3

2 http://www.theyworkforyou.com/lords/?id=2010-01-20a.1009.3&s=evidence+speaker%3A13450#g1026.3

that this protection should be provided by the initial obligations code.

> Arguably, subscribers are in at least as much need of protection against negligence on the part of copyright owners and internet service providers as are internet service providers in their relationship with copyright holders. I certainly concur with the noble Lord, Lord Howard, on that. However, this situation will not arise in practice. Subscribers will have a clear path to appeal at each stage of the process. The grounds of such appeals will certainly include the failure of the internet service supplier or the copyright owner to comply with the code or the copyright infringement provisions, or failure to observe the provisions of the Data Protection Act, which in any case contains its own penalties for failure to comply.[3]

Furthermore it is not clear how the QA process as established in the draft initial obligations code complies with the DEA requirement that: "the provisions of the code are objectively justifiable in relation to the matters to which it relates", "that those provisions are not such as to discriminate unduly against particular persons or against a particular description of persons", "that those provisions are proportionate to what they are intended to achieve" and "that, in relation to what those provisions are intended to achieve, they are transparent."

2.2 The code does not currently require evidence to be robust

The evidence gathering system needs to be robust and accurate as such the initial obligations code needs to define what constitutes a reasonably reliable evidence gathering system for the purpose of making allegations against subscribers under the DEA. The QA process proposed in the draft initial obligations code will require copyright owners and their agents to self certify that "in the reasonable opinion of the qualifying copyright owner, the process and systems described (in the quality assurance report) are effective in gathering robust and accurate evidence". Any copyright owner would do so, in fact ACS:Law and Davenport Lyons consistently claim that their evidence gathering process is robust, even though Which?, Consumer Direct, the Citizens Advice Bureau and the Solicitors Regulation Authority continue to receive complaints from subscribers who say they are wrongly accused.

Provision of a quality assurance (QA) report should not be a substitute for a baseline requirement that reasonably reliable evidence gathering systems should be used and proper evidence provided; the purpose of the QA report should only be to back up that requirement and enable checking of compliance with that requirement. If the processes and systems detailed in a QA report aren't in fact reliable, why should the mere provision of a report be enough to allow a Qualifying Copyright Owner to make (probably erroneous) CIRs against innocent subscribers? The draft initial obligations code does not require Ofcom to ensure that the evidence is reliable, though draft code (DC) 3.6 enables Ofcom to require changes to processes and systems.

But in the absence of a baseline requirement being established for the standard of evidence and the means to collect evidence it is not clear which criteria Ofcom would use for requiring changes to be made, and whether Ofcom will do so before any CIRs are sent out. Under the draft code the sending of CIRs based on unreliable and flimsy evidence is not punishable, ie. Ofcom has no means of enforcing any standard of evidence against qualifying copyright owners, and hence there is no barrier against the likes of ACS:Law using the Digital Economy Act.

If the initial obligations defined the standard of evidence required and the means of obtaining evidence for inclusion in a CIR, as required by the Digital Economy Act, Ofcom would have the power to enforce this standard against copyright owners as part of its powers to enforce compliance with the initial obligations code. But in its current form the draft initial obligations code does not ensure that CIRs sent out are based on robust and accurate evidence.

In addition to setting a baseline requirement Ofcom should include provisions in the code to the effect that CIRs which are based on an evidence gathering process that falls below the baseline requirement are automatic invalidated. As a result, any consequential notifications and/or inclusion in the Copyright Infirngement List would be deleted immediately.

---

3 http://www.theyworkforyou.com/lords/?id=2010-01-20a.1009.3&s=evidence+speaker%3A13450#g1026.3

2.3 No definition of the process by which customers are identified

The DEA also requires that Ofcom's Initial Obligations Code specify the means by which subscribers are identified by ISPs. For groups like ourselves, seeking to ensure that citizens' interests are properly protected, it is essential that we are given the detail required by the Act. Only by examining what is proposed can we comment on whether safeguards are actually present. Any comment on the sort of problems that may arise from different methods of evidence gathering is ultimately pure conjecture without a fully worked up code.

Section 7/124E(3) of the DEA requires that the initial obligations code create provisions covering the notification of subscribers for whom the internet service provider receives one or more CIRs. These provisions include "requirements as to the means by which the internet service provider identifies the subscriber".

In contrast, the QA process outlined in Section 4 of the draft code does not make "requirements as to the means by which the internet service provider identifies the subscriber", but instead only requires that the qualifying ISP complies with the process outlined in their own QA report.

The means by which subscribers will be identified will be extremely varied. They may be automated or manual. Public intermediaries may have very different processes. ISPs themselves may be reselling services to other ISPs. ISPs may be supplying internet access to public intermediaries.

The draft code in section 4.3 states that ISPs will not need to process a CIR if "the Subscriber using the IP address at the time of the alleged infringement cannot be reliably identified". Yet the code does not say what "reliably identified" might mean, as it does not define the standards of evidence required.

Furthermore it is not clear how the QA process as established in the draft code complies with the DEA requirement that: "the provisions of the code are objectively justifiable in relation to the matters to which it relates", "that those provisions are not such as to discriminate unduly against particular persons or against a particular description of persons", "that those provisions are proportionate to what they are intended to achieve" and "that, in relation to what those provisions are intended to achieve, they are transparent."

Following on from this, the process of identification and storing of information needs to comply with data protection laws, as we discuss below.

2.4 No provisions explaining how ISPs keep information about subscribers

The DEA requires that Ofcom's code makes provisions about how ISPs keep information about subscribers. This information is important in order that we are able to assess the privacy risks inherent in the storage of this data, including whether the information stored will be secure from tampering and misuse. Not being able to comment on this key element of the Initial Obligations Code is a serious problem for us.

2.5 Threshold for determining a 'relevant subscriber' is not set

The DEA requires that Ofcom's code sets a threshold of notifications made to a subscriber in relation to a copyright owner (Section 7/124E(1)(c)), in order that they are a 'relevant' subscriber whose details may be offered after a court order to the copyright owner. The code instead offers a scheme by which, after three notifications from the ISP, they are placed on a list (of "repeated infringers"). So the code sets a threshold for determining "relevant subscribers" in relation to notifications sent by ISPs and not CIRs received by ISPs. This does not comply with the DEA.

That Parliament expected thresholds to be set by the code was recognised in the debates:

> We absolutely accept that the concept of a threshold is important, and the Bill allows for it. Our approach to the threshold is that it should be for the code, but I recognise that this is not a sufficient answer. Let me say that we would expect the threshold to be based on the number of CIRs received over a period of time. The details should be left to the code. I accept that we must develop the concept of a threshold. We make

allowances for it in the Bill and we will put flesh on to the bones in the code. [4]

The very notion of a 'threshold' distinguishes it from the process of sending three notifications.

Instead of the approach mandates by the DEA and advocated by the government front bench, Ofcom have conflated CIRs and notifications sent to subscribers. We need to see the details of a fully functioning, compliant scheme in order to assess its fairness and efficacy by offering this non-compliant alternative, we are denied that opportunity.

2.6 No justifcation or explanation of data protection concerns

The entire process of collection and storing of data in this area is fraught. Personal copyright infringement is, ultimately, a matter between private parties and not something endangering state security or being a matter of serious crime: the type of infringement targeted not a crime, but a tort. Each copyright infringement notice may relate to a music file with a retail value as low as 35p, but is almost always a matter of small sums of money, not state or public security.

In general, the state should not therefore mandate data retention or mass surveillance for this sort of dispute between two private parties as it would endanger the human right to privacy (Article 8 of the ECHR). Such surveillance or data retention could only be justified on the grounds of serious crime or public danger. The case for keeping and using this data as evidence for a minor private offence is therefore most likely that it already exists for business purposes or under data retention requirements.

Yet in fact, to make this evidence reliable and useful given the scale of of people that may be targeted for low value infringements, a great deal of expense will have to be borne that has nothing to do with general business use, and new data retention obligations created. The Code should not be used to extend new obligations of data retention to, for instance, mobile operators, nor is it appropriate for the Code to be mandating new requirements for the standards of data collected. Data retention obligations should be dealt with openly through primary legislation and not through an SI targeting copyright infringement.

The case for collecting and storing information about private individuals on the internet by private parties needs to be set out. There are significant worries about such processes, recently outlined by European Data protection supervisors taking part in the Article 29 Working Group, echoing the European Data Supervisor's concerns about 'three strikes' schemes. These concerns should have been addressed in a privacy impact assessment, by Parliament, or now by Ofcom.

European Data Supervisor: IP addresses are personal data

Peter Hustinx's opinion, endorsed by the Article 29 Working group,[5] stated in relation to ACTA, makes it clear that in the view of the European Data Supervisor IP addresses are personal data in this circumstance:

> In the EDPS view, the monitoring of Internet user's behaviour and further collection of their IP addresses amounts to an interference with their rights to respect for their private life and their correspondence; in other words, there is an interference with their right to private life. This view is in line with the case law of the European Court of Human Rights.
>
> ...
>
> If one considers the definition of personal data provided in Article 2 of Directive 95/46/EC, 'any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number', it is only possible to conclude that IP addresses and the information about the activities linked to such addresses constitutes personal data in all cases relevant here. Indeed, an IP address serves as an identifi cation number which

4 Lord Young, 12 January 2010 http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100112-0011.htm

5 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2010_07_15_letter_wp_commissioner_de_gucht_acta_en.pdf

allows finding out the name of the subscriber to whom such IP address has been assigned. Furthermore, the information collected about the subscriber who holds such IP address ('he/she uploaded certain material onto the Web site ZS at 3 p.m. on 1 January 2010') relates to, i.e. is clearly about the activities of an identifiable individual (the holder of the IP address), and thus must also be considered personal data.

These views are fully shared by the Article 29 Working Party which, in a document on data protection issues related to intellectual property rights stated that IP addresses collected to enforce intellectual property rights, i.e. to identify Internet users who are alleged to have infringed intellectual property rights, are personal data insofar as they are used for the enforcement of such rights against a given individual.

Directive 2002/58/EC is applicable as well, as three strikes Internet disconnection policies entail the collection of traffic and communication data. Directive 2002/58/EC regulates the use of such data and provides for the principle of confidentiality of communications made over public communications networks and of the data inherent in those communications.

European Data Supervisor: intrusions into private communication need strong justifications, that show they are necessary and proportionate

Hustinx goes on to explain that measures of this nature - which would include this scheme from Ofcom – need to be clear about justitications for interference with privacy, which the EDS regards such monitoring to be:

Article 8 ECHR sets forth the principle of necessity pursuant to which any measure that infringes the right to privacy of individuals is only allowed if it constitutes a necessary measure within a democratic society to the legitimate aim it pursues. The principle of necessity can also be found in Articles 7 and 13 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The principle requires an analysis of the proportionality of the measure, which must be assessed on the basis of a balance of the interests involved, which is placed in the context of the democratic society as a whole. It furthermore implies an assessment as to whether alternative measures exist which are less intrusive.

Although the EDPS acknowledges the importance of enforcing intellectual property rights, he takes the view that a three strikes Internet disconnection policy as currently known — involving certain elements of general application — constitutes a disproportionate measure and can therefore not be considered as a necessary measure. The EDPS is furthermore convinced that alternative, less intrusive solutions exist or that the envisaged policies can be performed in a less intrusive manner or with a more limited scope. Also on a more detailed legal level the three strikes approach poses problems. These conclusions will be explained below.

The EDPS wishes to emphasise the far-reaching nature of the imposed measures. The following elements must be mentioned in this regard:

(i) the fact that the (unnoticed) monitoring would affect millions of individuals and all users, irrespective of whether they are under suspicion;

(ii) 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/EC which requires stronger safeguards;

(iii) 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;

...

(v) 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.

The EDPS is not convinced that the benefits of the measures outweigh the impact on the fundamental rights of individuals. The protection of copyright is an interest of right holders and of society. However, the limitations on the fundamental rights do not seem justified, if one balances the gravity of the interference, i.e. the scale of the privacy intrusion as highlighted by the above elements, with the expected benefits, deterring the infringement of intellectual property rights involving — for a great part — small-scale intellectual property infringements. As indicated by the Opinion of Advocate General Kokott in Promusicae: 'It is … 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'.

In this context, it is also worth recalling the European Parliament's reaction to 'three strikes schemes' in the context of the review of the telecoms package, particularly Amendment 138 to the Framework Directive. In this amendment it was laid down that any restriction to funda mental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the ECHR and with general principles of Community law, including effective judicial protection and due process.

In this view, the EDPS further underlines that any limitation to fundamental rights will be subject to careful scrutiny both at EU and national level. In this context, a parallel can be drawn with the Data Retention Directive 2006/24/EC, which derogates from the general data protection principle of deletion of data when they are no longer necessary for the purpose for which they were collected. This directive requires that traffic data are retained for the purpose of combating serious crime. It has to be noted that retention is only allowed for 'serious crime', that the retention is limited to 'traffic data' which in principle excludes information about the content of communications, and that stringent guarantees are adduced. Nevertheless, doubts have been raised on its compatibility with fundamental rights standards; the Romanian Constitutional Court decided that blanket retention is incompatible with fundamental rights, and there is currently a case pending before the German Constitutional Court.[6]

Ofcom needs to justify these intrusions into private communications

This second part of Hustinx's opinion is espcially important regarding Ofcom's duty under the Act to show that 'the provisions of the code are objectively justifiable in relation to the matters to which it relates' and 'that those provisions are proportionate to what they are intended to achieve'. In any case, the severity of impacts of private moitoring clearly should be subject to a privacy impact assessment, and the justifications should be set out prior to this or a future consultation.

The reasons why personal data may be processed are called "conditions for processing" under the Data Protection Act. The Code should set out what the justifications are.[7] These conditions need to be set out for both the private parties and the ISPs databases of infringement allegations.

The code fails to explicitly state whether the subscriber's data and IP address are sensitive personal data under the Data Protection Act 1998. IP addresses and other personal data relating to the subscriber consist of information as to: "any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings." This is extremely important, as this affords greater standards of protection and access.

In particular, we urge Ofcom to assess whether the draft initial obligations code, which is to become secondary legislation, complies with the relevant EU data protection and data retention directives. Unfortunately the UK Government has failed to properly implement EU data protection and retention standards into UK law, therefore we ask Ofcom to assess compliance with EU standards, not just UK law on the matter. In particular we are concerned that the draft initial obligations code places a duty on internet service providers to retain IP logs for the purpose of matching CIRs to subscriber details for 10 days, and Ofcom needs to ensure that this complies with relevant EU data retention standards.

6 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:EN:PDF

7 http://www.ico.gov.uk/for_organisations/data_protection_guide/the_conditions_for_processing.aspx

We are also concerned that the draft initial obligations code does not make the deletion of CIRs by the ISP an absolute requirement, instead Section 5.2 of the draft initial obligations code states that: "As far as is reasonably practicable, the Qualifying ISP must retain this information for no longer than 12 months after receipt of the CIR in question." Ofcom should clearly state that the CIRs need to be deleted after 12 months, failure to do so would then be a non-compliance with the initial obligations code.

We also ask Ofcom to clarify how anonymity of notified subscribers will be ensured at all stages of the process.

2.7 Content of notifications needs standardisation, as required by the Act

Parliament, in the debates, recognised that the content of notifications was very important. They therefore made an effort to specify some of the content of such notifications, and required Ofcom's code to standardise that information.

Subscribers will rely on the information provided to them in the notifications to bring their "subscriber appeals" and as such it is welcome that Section 5.11(c) of the draft initial obligations code requires the notifications to include all evidence that is included in the copyright infringement report in a standardised format, that is: (draft initial obligations code 3.3)

(a) the name and registered address of the Qualifying Copyright Owner;
(b) where relevant, name and registered address of the person on whose behalf the Qualifying Copyright Owner is authorised to act and evidence of authorisation;
(c) identification of the work in which copyright in the UK is said by the Qualifying Copyright Owner to subsist (the "Relevant Work"), including the title of the Relevant Work and a description of the nature of the Relevant Work;
(d) a statement that there appears to have been an infringement of the owner's copyright in the Relevant Work;
(e) a description of the apparent infringement, including the filename, a description of the contents of the file, and (where appropriate) hash code of the infringing content;
(f) a statement that, to the best of the Qualifying Copyright Owner's knowledge, no consent has been given by the owner of the UK copyright in the Relevant Work for the acts described in the preceding paragraph to have occurred;
(g) the date and time using Universal Coordinated Time (UCT) on which the evidence was gathered, including both the start and end time of the relevant session; (h) the IP address associated with the apparent infringement;
(i) port number used to conduct apparent infringement;
(j) the website, or protocol, via which apparent infringement occurred;
(k) a Unique infringement identifier (UII) allocated to the CIR by the Qualifying Copyright Owner; and
(l) the date and time of issue of the CIR.

However, the draft initial obligations code fails to standardise information to be given to subscribers. The DEA requires the following information "about subscriber appeals and the grounds on which they may be made" to be standardised:

"information about copyright and its purpose"

"advice, or information enabling the Subscriber to obtain advice, about how to obtain lawful access to copyright works"

"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".

The draft initial obligations code also incorrectly requires all notifications to include information about:

"the ability of a Qualifying Copyright Owner to bring a legal action for damages in relation to an infringement".

This is not a requirement of the DEA. It is also factually incorrect. A copyrights owner can bring an action against a subscriber for infringement, and in some circumstances, if found guilty, the court may award damages. Unlike the DEA provisions, an infringement action would be required to link the infringement to the subscriber.

In a similar vein, the draft code requires that "advice, or information enabling the Subscriber to obtain advice, about reasonable steps that the Subscriber can take to protect an internet access service from unauthorised use" be given, in line with the DEA, but goes on to require information be given as to how to:

"prevent online copyright infringement in the future"

– an impossible task. The DEA more realistically requires "advice on securing internet access services against unauthorised use".

We would like these elements to be properly corrected so that we can consider the content of notifications properly.

2.8 Appeals are misimplemented, requiring stronger burdens of proof on subscribers than the Act requires

The Appeals process also contravenes the process set out the DEA.

Section 13/124K(3) and (6) of the DEA provides that the initial obligations code must provide that if a subscriber appeals on the grounds that "the apparent infringement to which the report relates was not an infringement of copyright" or "that the report does not relate to the subscriber's IP address at the time of the apparent infringement", the appeal must be determined in favour of the subscriber if the subscriber shows that "the act constituting the apparent infringement to which the report relates was not done by the subscriber" and "the subscriber took reasonable steps to prevent other persons infringing copyright by means of the internet access service".

The two relevant ground for appeals mentioned in the DEA are specified in Section 7.12.1 and 7.12.2. Overall the draft initial obligations code provides for five grounds of appeal in sections 7.12.1 to 7.12.5. In section 7.24 the draft initial obligations code then provides that "where a Subscriber Appeal contains a ground set out in paragraph 7.12.1, 7.12.2, 7.12.3, 7.12.4 or 7.12.5 a Subscriber Appeal must be determined in accordance with 7.22.1 if the Appeals Body is satisfied that the Subscriber has shown that, in relation to a relevant CIR: 7.24.1 the act constituting the apparent infringement to which the CIR relates was not done by the Subscriber, and 7.24.2 the Subscriber took reasonable steps to prevent other persons infringing copyright by means of the internet access service."

It appears from the draft initial obligations code that an appeal on any grounds can only be upheld if the subscriber proves that "the act constituting the apparent infringement to which the report relates was not done by the subscriber" and "the subscriber took reasonable steps to prevent other persons infringing copyright by means of the internet access service". The DEA only requires that the subscribers proves the above two cases where the appeal is in relation to either "the apparent infringement to which the report relates was not an infringement of copyright" or "that the report does not relate to the subscriber's IP address at the time of the apparent infringement". Hence the draft initial obligations code places a considerable burden of proof on the subscriber which is not required by the DEA.

Section 13/124K(5) of the DEA also requires that the initial obligations code "must provide that an appeal on any grounds must be determined in favour of the subscribers unless the copyright owner or internet service provider shows that..." "the apparent infringement was an infringement of copyright" and "the report relating to the subscriber's IP address at the time of the infringement". However the draft initial obligations code does not fully implement these DEA requirements. Section 7.23 of the draft initial obligations code states that "a Subscriber Appeal on any grounds may only be determined in accordance with paragraph 7.22.2 (must be rejected) if the Appeals Body is satisfied that there is sufficient evidence to show that, as respects any CIR to which the Subscriber Appeal relates or by reference to which anything to which the Subscriber Appeal relates was done (or, if there is more than one such CIR, as respects each of them): 7.23.1 the apparent infringement was an infringement of copyright, and 7.23.2 the CIR relates to the Subscriber's IP address at the time of that

infringement. " In doing so the draft initial obligations fails to implement the clear requirement for an appeal on any ground to be determine in favour of the subscriber (that is upheld) unless the copyright owner or the internet service provider can prove that "the apparent infringement was an infringement of copyright" and "the report relating to the subscriber's IP address at the time of the infringement". The Section 13/124K(5) requirement is of utmost importance because it means that an invalid CIR or failure by the internet service provider to accurately match the IP address would automatically mean that the subscriber appeal is upheld in favour of the subscriber.

Section 13/124K(7) of the DEA also requires that "where the appeal is determined in favour of the subscriber, to direct the copyright owner or internet service provider to reimburse the reasonable costs of the subscriber". In section 7.28 the draft initial obligations code states that the appeals body may only award such costs "unless it is satisfied that it would be unjust to give such direction having regard to all the circumstances including the conduct of the parties before and during the proceedings." This is not required by the DEA and it is unclear why the right of the subscribers to have reasonable cost reimbursed is limited in this way. It is also not clear what Ofcom has in mind in relation to the reimbursement being "unjust", a term that is not defined in law or the consultation document.

Furthermore we are concerned that the draft initial obligations code does not provide subscribers with the option of appealing against the decision reached by the Appeals Body or what subscribers should do if they think the Appeals Body has not complied with the initial obligations code in reaching their decisions. Presumably they can complain to Ofcom regarding the Appeals Body's non-compliance with the initial obligations code, but if this is the case it needs to be made explicit.

2.9 Definition of "copyright owner" is incorrect and could lead to incorrect advice, privacy abuses and unfair release of personal data

The draft initial obligations code and the Act state that a "Copyright Owner" means "(a) a copyright owner within the meaning of Part 1 of the Copyright, Designs and Patents Act 1988 (see section 173 of that Act); or (b) someone authorised by that person to act on the person's behalf".

It is likely that agencies such as Logistep, Trident Media Guard or DtecNet will be hired to act as agents under the (b) definition, since they have the technology for tracking file sharing. Additionally, numerous major copyright owners may band together under the umbrella of the British Phonographic Industry (BPI) or the Motion Picture Association of America (MPAA), who may then act on their own account, or may appoint specialist agents themselves.

It seems quite possible that at one time or another, all of these different types of organisation will be issuing CIRs, and indeed might even all detect the same activity at the same time. We do not believe that Ofcom have properly considered the ramifications of this.

The Digital Economy Act says 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". This wording is repeated in the Code (albeit with the restriction that it must be a Qualifying Copyright Owner). But there is an unexpected problem lurking here for the provider (the ISP) because they may now have to tie together CIRs from multiple sources which refer to the same "owner".

That may be an unpleasant surprise to the provider if they have not designed their database correctly, especially if Ofcom requires them (as they should) to amalgamate/discard multiple reports (from multiple "copyright owners") for the same event.

The current wording may also provide an unscrupulous "owner" with a way of evading the rate limiting in #6.6 of the Code (especially because the payments and estimates of volume involved in becoming "Qualified" do not apply to requests for infringement lists). They need only to appoint multiple agents (who will generate no CIRs) and they can make as many requests as they wish. Since the Code is constrained by the wording of the Act, this may be difficult to resolve -- but one simple way ofaddressing it, and fixing the database issues, would be to ensure that infringement lists should only deal with CIRs submitted by the entity asking for that list.

However, the problems are not yet over. Where a "copyright owner" is in fact an agent acting for multiple actual owners, they may be able to tie together information within multiple infringement lists (which are intentionally anonymous) with de-anonymised data from a single court action. This is quite clearly against the intentions of Parliament as regards how the Act should operate. The Code must add appropriate wording to #6.4 to ensure this cannot occur.

However, there is a much more elegant and straightforward way of dealing with these issues. We note that s124B(1)(b) permits Ofcom to use the Code to limit access to copyright infringement lists. We strongly recommend that the Code should require that only an actual copyright owner (ie: the CDPA 1988 definition) may request the copyright infringement list, and the database issues should be addressed by making it explicit in the Code that the provider (the ISP) will need to match the actual owners name and address (ie the data supplied in #3.3(b) not in #3.3(a)) when it creates such a list.

The problems with the owner terminology occur in several other places as well because the current draft initial obligations code does not clearly distinguish between the actions that can be taken by the "copyright owner" as defined by the initial obligations code, and the "copyright owner" as defined in the Copyright, Designs and Patents Act 1988.

This is particularly important because the Code has "copied in" the text in the Digital Economy Act that "the copyright owner may apply to a court to learn the subscriber's identity and may bring proceedings against the subscriber for copyright". However, under UK law only the actual copyright owner as defined in the Copyright Designs and Patent Act 1988 can apply for such a court order. An agent would not be able to do this. The Code should not purport to indicate otherwise by sloppy use of precise language.

The text at #5.13.3, #5.14.4, #5.15.3 and #5.16.3 (at the very least) will need to be changed to remove the false statements currently present.

To make this clear, the Code must make it clear throughout that a company such as Logistep, Trident Media Guard (TMG) or DtecNet could act as "copyright owner" to make infringement reports under the Act; but the Code should ensure that they cannot request copyright infringement lists and should make it crystal clear that they certainly cannot (whatever s124A(8)(c) purports to say) apply for a court order to gain the details of infringing subscribers under the Copyright Designs and Patent Act 1988.

2.10 Ofcom must explain how their code meets the Act's criteria for approval

Section 7/124E(1) of the DEA establishes a set of criteria and Ofcom must not approve the initial obligations code unless it is satisfied that it meets the criteria set out in this section. The criteria for approval of the initial obligations code are:

- 'the provisions of the code are objectively justifiable in relation to the matters to which it relates'
- 'that those provisions are not such as to discriminate unduly against particular persons or against a particular description of persons'
- 'that those provisions are proportionate to what they are intended to achieve'
- 'that, in relation to what those provisions are intended to achieve, they are transparent'

While the consultation document references these criteria in relation to its decision to not implement some of the DEA requirements, particularly in relation to not complying with Section 5/124C(5) requirement for the Code to set a threshold for qualifying ISPs based on the number of CIRs received, Ofcom has provided no overall analysis on whether the draft initial obligations code meets the criteria set out above.

In relation to transparency, any directions and guidance Ofcom or the Appeals Body may provide to qualifying copyright owners or internet service providers once the initial obligations code has come into force need to be made public and communicated to subscribers who are notified under this scheme.

2.11 WiFi operators still face problems and the Code could lead to closure of networks

We are greatly concerned that the proposals made in the consultation document would not allow Wifi to continue to be offered as normal, be it password protected or open.

The definition of "subscriber" and "internet service provider" provided in the draft initial obligations code create a number of problems, particularly in relation to other definitions provided in the consultation document itself. For example, in relation to the definition of subscriber, the draft initial obligations code states that the internet access service must be provided under agreement. But the consultation document states that a user of a WiFi network would only be a subscriber if the internet access service is provided under explicit or implicit agreement and in return for payment.

But this definition is not contained in the draft initial obligations code. If the definition in the draft initial obligations code was applied to users of WiFi, all users of WiFi, including open Wifi, would be subscribers as they all receive it under an explicit or implicit agreement. In turn, because the draft initial obligations code defines "Fixed ISP" as any ISP who "provides a fixed internet access service", all providers of WiFi would be Fixed ISPs. But the consultation document states that Wi-Fi operators may only be classified as ISP if there is payment, if there is no payment the operator of the WiFi network is a subscriber.[Draft initial obligations code, Section 1] This definition is not in the draft initial obligations code and it is not clear what Ofcom is actually consulting on.

In any case, the definition outlined in the consultation document creates significant problems for operators of wifi networks. The consultation document states that wifi operators providing internet access service on agreement, explicit or implicit, and against payment, are to be "internet service providers" and wifi operators who provide internet access service without any payment are to be classified "subscribers", meaning that any open or free wifi will be classified as subscriber for the purpose of the act.

This means that especially public intermediaries such as libraries and councils, who frequently provide open and free WiFi access to users, would be classified as subscribers, and therefore copyright owners may make copyright infringements reports against them. As these operators are put on copyright infringement lists, they would be subject to court action by copyright owners and to technical measures if those are introduced at a later date.

Open WiFi provided by not for profit organisations and public intermediaries plays a key role in providing internet access to all users. For example Islington council provides a free WiFi hotsport, called StreetNet, on Upper Street and Holloway Road near Angel tube station, which provides registered users with free one-hour session (i.e. no payment is required).

Classifying wifi operators who provide the service against payment as "internet service providers" does not necessarily make them immune from the provisions of the act either. That is because the draft initial obligations code provides that any "internet service provider" with more than 400,000 subscribers will be a qualifying ISPs. Ofcom fails to consider that some paid for wifi operators may well provide access to more than 400,000 users. For example, The Cloud, which provides WiFi against payment in the City Of London reportedly allows "more than 350,000 people who work in and visit the area access to wireless broadband." The Mayor of London now plans to role out a similar service across London, stating that "London is the home of technological innovation. We in City Hall are doing our best to keep up, and one of our most important projects is called wi-fi London". BBC It is not clear whether Ofcom considers service such as The Cloud as qualifying ISP, especially if such services were roles out London wide, potentially providing access to millions of people.

Therefore Ofcom has failed to clarify the position of wifi operators and its suggested approach is likely to cause great uncertainty for wifi operators, which may be consumers, businesses or public intermediaries.

2.12 Summary of problems

- The code is incomplete in terms of DEA requirements
- The code has errors in its implementation of the DEA

- Ofcom does not explain how its code does not explain how it fulfils the criteria set out by Parliament in the DEA
- Without this information, we cannot properly contribute to the consultation, Ofcom therefore needs a further round with a new draft code without these errors and omissions.

3 Specific problems with the code other than non-compliance with the DEA

3.1 Effect of CIRs on future technical measures and the failure to warn about consequences of a CIR

The DEA makes no distinction between CIRs issued in Stage 1 and Stage 2. The result is that a CIR issued in Stage 1 may have the effect of triggering 'technical measures in stage 2. As the Draft Code stands, subscribers will not be warned that this is the case. Ofcom have verbally stated to ORG that they regard the two stages as separate, but in legal terms, this is not so. After a year, Ofcom will report to the Secretary of State, and at any time after that, 'technical measures' may be imposed. At some point in the first year, therefore, potential for people receiving CIRs to be punished under Stage 2 exists.

The simple 'natural justice' point to make is that people need to be warned of the consequences of their actions. In this case, someone who does not protect their network, and receives a CIR may find this leading to technical measures once this stage is introduced. Furthermore, the handling of the serious infringer lists needs clarity. These subscribers are under the most serious risk of undue disruption, which they need to be informed about.

We do not wish to over-extend these problems. We do not wish for Ofcom to create additional pressures for the closing open wifi networks, or to issue advice while there is no potential for overlap. But once this potential exists, then advice does need to be given, and the Draft Code should reflect this.

Ofcom may argue that they do not know if CIRs will count in possible Stage 2 technical measures, and that this is an issue for the Secretary of State and Parliament to decide in secondary legislation. They may say have no remit at the moment to do anything in this area. However, the legislation already creates these possibilities.

We would like to know if the draft SI could create a barrier between the two stages, or if the government could indicate that Stage 1 notifications would not count in Stage 2. This issue however has not been dealt with in this consultation, and we would again like to see a second consultation that gives some clarity on these points.

3.2 Advice to subscribers

The Code should provide for means to create independent advice for subscribers receiving CIRs. We assume Consumer Direct and Citizens Advice will both need financial help to deal with new workload created by notifications. The Code should allow for fees from the process to pay for this.

3.3 Subscriber Appeals

Appeals are a critical area. As we note above, the grounds suggested do not comply with the Digital Economy Act. Section 7.2 is also missing a number of potential circumstances that should be taken into account.

These range from technical illiteracy, a problem that may affect new users and some parts of the older population, through to technical difficulties.

In our informal conversations, Ofcom seemed to be of the view that providers of open wifi could effectively restrict the activities of their clients. This is not the case. If a user has full control of their machine, they can use any number of means to prevent firewalls and port blocking from working.

There are also many circumstances where it is harder because P2P technologies are part of the legitimate activities of their users. We therefore suggest defences being added to include that a subscriber had limitations to the 'reasonable measures' they could take for business or education reasons.

A subscriber might also open their wifi for other reasons, such as allowing people to send communications during a period of emergency, or during a community event. We therefore think there should be a defense of acting in the public interest defense as part of community events, incident responses, and so on.

Specific missing defences

Defences should include:

- That the user is a provider of an open wifi network, or community network, and 'reasonable measures' to secure Wifi are necessarily very limited
- That the user cannot prevent use of bit torrent technology as use of the technology forms part of their work or education
- That the user did not infringe copyright

3.4 Evidential requirements of Copyright owners and ISPs

This is the hardest for us to comment on. As we note above, the draft code is not in compliance with the DEA as it fails to set out standards for the evidence collected by copyright owners and retained by ISPs. The draft code omits all the important information about evidential standards, instead passing these to the copyright owners and agents, and the ISPs to self-authenticate.

DC 3.5 must be amended to insist evidence and collection systems are robust and accurate, for instance to read:

> "The evidence of copyright infringement to be included with CIRs must be robust and accurate, and each Copyright Owner must ensure that the means used to obtain evidence on its behalf must be such that the evidence meets that minimum standard."

In summary:

- The code must comply with the DEA requirement to specify the evidential methods of producing CIRs
- The code must comply with the requirement to define methods of identifying subscribers matching a CIR within the ISP
- The code must comply with the requirement to define methods of retaining accurate data about subscribers within the ISP

4 Answers to Ofcom's own 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.

We certainly agree that Copyright Owners should have to abide by the Act in order to use these procedures. However, the code omits to detail these procedures as we outline above, and therefore itself fails to comply with the Act.

We also note a conflation between a 'copyright owner' and a 'copyright Owner's agent. It may be that all music copyrights held by the four major labels, plus the major independents, plus many owned by film makers, and even those by major software houses, are handled by one agent. This distorts the meanings set out in the Act.

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.

NA

Question3.3: 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?

As we detail above, the draft code does not contain information detailing how evidential

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

NA

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?

NA

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?

Ofcom seems to have abolished the category of Communications Providers. We are not certain this complies with the Communications Act. Without setting out a means for a Communications Provider to seek to exempt themselves from the code, by an ISP identifying who they supply internet access to as a 'communications provider', the Code may drag organisations into the Act for no good reason. We note Communications providers have significant legal obligations and it is unlikely groups will seek to become a Communications provider in order to escape the DEA's obligations.

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?

It is clear the content needs to be standardised,

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.

We do not believe this approach is compatible with the Digital Economy Act, which requires the draft obligations code to require defined standards and means of collecting evidence. We detail our concerns above.

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?

Subscribers should have the right to receive CIRs immediately. Subscribers should also have the right to access information collected about them by third party agencies. As mentioned above, this is a fraught area, which raises considerable concerns among data protection agencies across Europe, and may breach privacy rights. A fully detailed explanation of how this will operate and privacy impact assessment should be part of this consultation.

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.

We note above problems with disposing invalid CIRs and making sure these do not result in difficulties with appeals.

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.

As we note above, this process does not comply with the Digital Economy Act, which requires this Code to detail "requirements as to the means by which the internet service provider identifies the subscriber" in Section 7/124E(3). Leaving this entirely to the ISP to determine is both non-compliant and prevents us from commenting on the appropriateness of Ofcom's non-proposal.

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.

As we note above, the proposal is not compliant with the DEA. It conflates notions of copyright owner's agents and the actual copyright owner. It conflates notions of CIRs and notifications and mis-implements the serious infringers' lists, as well as mis-implementing the means by which a copyright owner may access the list.

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?

As we note above, the draft code fails to comply with the Digital Economy Act's requirements for the content of notifications, by ignoring some requirements and misrepresenting others. Standardised information is important and required by the Act.

The draft illustrative notifications are very badly drafted and do not properly represent copyright law or the Digital Economy Act's provisions.

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.

As we note above, the Draft Code has not properly implemented the threshold provisions of the Digital Economy Act. Thresholds are meant to be related to the number of CIRs issued relating to actual copyright owners. In contrast, the Draft Code's model is based on the total number of letters sent to all copyright owners, and additionally conflates actual copyright owners with their agents.

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.

As we note above, the Draft Code's provisions on subscriber appeals fails to comply with the Digital Economy Act. We also detail specific extra defences that are needed to allow people to use bit torrent technologies for business and education without fear of wrongful accusation. We note that it is not the aim of the code to prevent use of the technology but to target infringement.

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.

We are particularly critical that no real incentives are created to make sure that evidence gathering is robust, nor that ISP records are accurate. We have not examined this section for compliance with the DEA.

5 Bringing Ofcom's work back into line with their broader objective and those of the DEA

Ofcom have a wider duty to "further the interests of citizens and of consumers" and harness the benefits of competition in the communications sector. This code is likely to damage the interests of many citizens, and reduce competition in the communications sector. We have concentrated on the areas that are likely to damage citizens' interests, centring on those points that may create bad judicial decisions, and hamper legitimate activity such as providing and sharing wifi access.

However, while concluding we feel compelled to remind Ofcom that this system loads the dice against smaller distributors, individual copyright holders, innovative legal services using peer-to-peer technology, and stresses the need for individuals, orgainsations and businesses to close off legitimate technologies or face possible liabilities. In the round, this is likely to produce substantial costs and harm, and Ofcom should be mindful to collect evidence of this harm in order to understand the effects of this Act.

6 Summary: another round of consultation is needed

We have at present a broken implementation of the DEA to look at. It has proven impossible to give sensible feedback on standards of evidence and data because the requirements are simply absent, and replaced by yet another attempt to pass the buck, in this case, to the ISPs and rights holders. As a citizen group, we find this outrageous.

We do not, however, think this is Ofcom's fault. For a start, Ofcom have been given a ridiculous timetable by the new Act, and created their draft code in a matter of weeks, rather than months.

Ofcom is legally bound to give Parliament a working Code to create a draft instrument. Ofcom is also legally bound to consult with the public. But the high level errors that have resulted from the truncated timetabling mean we have not been consulted on a working draft, but are looking at something that could not possibly be put before Parliament. We urge Ofcom to apply for further time to properly consult on a re-worked draft code.