Response to OFCOM Consultation: 'Online Infringement of Copyright and the Digital Economy Act 2010 - Draft Initial Obligations Code' published 28 May 2010.
Date of Response Submission: 15 Jul 2010

1 Statement of interest

1.1 This response is submitted on behalf of BeingThreatened.com, a consumer support website founded to support innocent people caught up in legal action initiated by ACS:Law, and previously Davenport Lyons, on behalf of rights holders for alleged file sharing activity. Many thousands of people have received demands in the region of £500[1], with the prospect of legal proceedings being lodged against them. It is stated in the first letter that, if they are found liable for the infringement they may end up being responsible for legal costs amounting to thousands of pounds, although to this date the quality of evidence held against them has not been tested in a court of law, or by any other independent party. This method of demanding money en-masse has turned the attempts to maintain the rights of copyright holders into a way to quickly profit from filesharing actions that may not even have occurred.

1.2 We have considerable concern at the number of misidentified people caught up in this legal activity and can only see this continuing despite the Digital Economy Act (DEA) and OFCOM's draft guidelines for the application of sections of the new legislation. It is of considerable concern that even if the guideline improves the requirements for evidential robustness, copyright owners may see fit to continue to send threatening letters paying no heed to the legislation or guideline[2]. Whilst OFCOM cannot prevent this, they can provide considerable influence as we will address in our response.

1.3 Whilst our response represents our opinions of how the consultation must be altered, many of our suggestions are both necessary and fundamental to the continuance and enforcement of due process in application of the law. This is clearly evident in the cases of those we support, where in many cases the evidence is based solely on a single instance of an IP address being spotted in a filesharing swarm, with no other information provided even on repeated request.

2 Responses to OFCOM's specific questions

2.1 *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.*

2.1.1 We agree it is vital for Copyright Owners to have a right to remedy under the Act. As set out further in responses to OFCOM's questions, and in our own additional comments, we hold this opinion with some reservations. In our experience some Copyright Owners have so far acted with considerable contempt to claims of innocence and have not demonstrated sufficient concern at the lack of rigour in the chain of evidence put forward to support their allegations[3].

2.1.2 We do not consider it essential to limit those able to take advantage of the provisions of the act to provide up front payment and numbers to an ISP before notifying the ISP of instances of infringement. Indeed, smaller rights holders may be encouraged to do so outwith the Act if they cannot reasonably give numbers or pay in advance. Discouraging rights holders from following the DEA, when the alternative appears to be untargeted

[1] http://www.which.co.uk/news/2010/01/acs-law-letter-writing-continues-197714/
[2] http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100126-0002.htm#100126-0002.htm_spnew26
[3] http://news.bbc.co.uk/1/hi/technology/8481790.stm

legal threat would be concerning to consumers. The concern therefore follows not from those able to take advantage of the act, but those who would continue to act outside of it in an inappropriate manner not compliant with the measures on evidential rigour we propose should be included in the code.

2.2 *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.*

2.2.1 No view

2.3 *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?*

2.3.1 Our sole concern on this point is that this approach will lead to no other remedy for rights holders when pursuing infringers on small ISPs. As mentioned previously, this may lead to a continuation of the ACS:Law style action of legal threats on poorly based evidence being used to pursue alleged infringers on the basis of a single monitoring instance outside the scope of the DEA. We do agree widely with OFCOM's approach, but request that appropriate consideration is given to these unintended consequences of leaving ISPs out of scope.

2.4 *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?*

2.4.1 No view

2.5 *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?*

2.5.1 We believe that the definition given within section 3.22 of the consultation is unnecessarily broad. An oral agreement would suggest that allowing temporary usage of a wireless network by a friend would automatically lead to the classification of that provision as internet service provision under the OFCOM definition. This would only serve to muddy the waters as to whether an individual subscriber also classifies as an ISP for the purposes of notification, despite the clarification that this would not apply where payment was not a constituent part of the agreement.

2.5.2 Specifically, the position would lack clarity where multiple parties shared a connection and the subscriber was paid by other users in a sub-let type agreement. This approach is common in student households where the bill-payer would divide the bill by the number of parties and may thus classify as an ISP under the OFCOM definition.

2.5.3 Of further concern is that the definitions within the consultation report omit mention of non-commercial access provision. This is a group which encompasses a range of public services such as non-residential (i.e. no private access provision) educational institutions and libraries. It would be concerning if these organisations were to hold liability at a subscriber level, as their service mandate is open access to all-comers. We would welcome OFCOM's clarification on this point and appropriate consideration to be given to this area in the final code.

2.6 *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?*

2.6.1 Although we broadly agree with OFCOM's interpretation of subscribers and communications providers, we feel strongly that the approach favoured by OFCOM may impact unfavourably upon organisations and individuals. Specifically if non-profit organisations such as schools and libraries are included, the Act may lead to a significant reduction in free internet provision such that the government's targets for internet access provision may suffer adversely.[4]

2.6.2 Notably the cited example within the consultation document of a subscriber providing free access to the local community would become untenable. Whilst the legislation may not explicitly state as such, there is now as part of the legislation and the proposed code a dangerous expectation that all wireless access is secured. This will lead to a reduction in portability of internet connection and would potentially question schemes such as BT Fon, especially where these are not provided via a secure VPN which can separate subscriber traffic from the Fon users. The government openly admitted at drafting that these concerns could come to fruition.[5]

2.6.3 We consider the implication that the wireless network operator has an implicit obligation to secure the network to be an extremely dangerous one. Ignoring the fact that putting in place technical measures is beyond some end users, and further that some older infrastructure may be incapable of reasonable security, it should be noted that all widely provided security methods provided in wireless equipment have been broken. Indeed both WEP and WPA encrypted connections are easily accessed in less than a minute, and WPA2 is accessible with a longer period of attack. Ruling out this potential for attack by assuming the level of security provision is sufficient will result in a number of people mistakenly receiving CIRs with no valid defence of wireless intrusion (which may have been the case despite the security measures taken).[6,7]

2.7 *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?*

2.7.1 We would suggest that in the example of letter three in the annexes, the date of first infringement is added in addition to the date of second infringement to allow paperwork traceability.

2.7.2 As we will elicit further in our response to the relevant question below, we consider it absolutely essential that the consumer is not misled that the sole evidence against them is an IP address. It is, in our view, mandatory to include reports that guarantee efficacy of the evidence provided by both the ISP and the data monitor with each request. These must be sufficiently detailed to describe the entire process as we shall further discuss below and posted for public scrutiny.

2.7.3 We are concerned that the FAQ contains a question related to preventing unauthorised access to a wireless connection (Question 15, page 74 of the consultation), yet fails to provide advice for unauthorised access where security measures have already been applied to the network (i.e. security beyond encryption).

2.8 *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.*

[4] http://www.eweekeurope.co.uk/news/digital-economy-bill-threatens-public-wifi-hotspots-5573
[5] http://www.openrightsgroup.org/assets/files/pdfs/bis/B2_-_Libraries,_Universities,_and_Wifi_Providers-Factsheet.doc
[6] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.926&rep=rep1&type=pdf
[7] http://wirelesscenter.dk/Crypt/wifi-security-attacks/Practical%20Attacks%20Against%20WEP%20and%20WPA.pdf

2.8.1 We fully agree that a highly quality controlled approach is necessary to define and maintain standards within the evidence gathering sector. Our experience with ACS:Law and their monitors, NG3 Systems, Logistep and Digiprotect, betrays a lack of transparency and independent quality control. Openness is a major factor when presented with an accusation that could eventually lead to court (however distantly). Our first request would therefore be that all documents submitted to demonstrate robustness and accuracy of evidence are immediately released into the public domain. Due to the nature of the allegations made by the data monitors it is entirely unreasonable to extend any sympathy for commercial exemptions for evidence disclosure.

2.8.2 We are concerned that OFCOM will present rights holders and evidence collection agencies with the ability to self-certify as to data gathering accuracy. Our experience with the activities of ACS:Law, their clients and data monitors indicates a worrying lack of concern at the apparent high false positive rate amongst their claims. At the date of submission of this response the number of individual complaints to the Solicitors' Regulation Authority against ACS:Law exceeds 400. There have also been several widely publicised cases where the evidence has been called into question via demonstration and the case dropped[8]. The pay up rate is estimated to be in the region of 20-40% dependent on the work that is alleged to have been shared[9]. We would estimate that the false positive rate in these cases is in excess of 25% of the letters sent. This is entirely unacceptable.

2.8.3 We have also found that despite asking for the evidence numerous times across several hundred people, including by invocation of clause 8 of Part 36 of the Civil Procedure Rules (which requires clarification of an offer for settlement; in this case relevant as it is impossible to assess the basis of an offer without evidence of the allegation), ACS:Law have manifestly refused or ignored these requests[10]. We can only conclude that the expert reports and evidential dossier contains sufficient flaws that release to the general public would immediately remove any potential for their clients to win a case in a court of law.

2.8.4 Of considerable concern is the following paragraph within the consultation report: *"This list is based on the information currently produced by agents working on behalf of Copyright Owners. We believe that this matches the standard of evidence required by the courts in relation to civil proceedings by Copyright Owners for copyright infringement. "*; we are apprehensive that the information provided in this section is related to ACS:Law's activities, as they are the only solicitors currently acting for Copyright Owners in pursuit of individual sharers today. The latter part of the quote is completely incorrect. The way ACS:Law operate is to pre-agree with ISPs that the service provider will not contest the court order. In doing so the evidence provided to the court is untested, and the rigour unknown. Without contention there is no basis to conclude that the evidence is sound, indeed where an ISP has stated intent to contest the order (notably TalkTalk) they have been dropped from inclusion in any future order[11]. Again, we can only conclude that ACS:Law is avoiding disclosing their full position and that the evidence must have clear flaws for them to continue this practice.

2.8.5 We believe that the approach OFCOM favours could offer a strong platform from which to improve evidence gathering techniques. Specifically best practices must be shared amongst the data monitors to improve the accuracy and false positive rate amongst the monitors. There is no excuse for one monitor to have a worse record at false allegations than any other monitor.

2.8.6 Whilst we believe that the list of minimum requirements set out in the consultation is a good start we will repeat here our list submitted as part of the BIS consultation on illicit filesharing last year, which we believe to be the minimum list of requirements for robust evidence:

[8] http://news.bbc.co.uk/1/hi/technology/7697898.stm
[9] http://www.bbc.co.uk/iplayer/episode/b00kn0kn/You_and_Yours_03_06_2009/ (18:18 onwards)
[10] Annex 2
[11] http://www.guardian.co.uk/technology/2010/feb/04/australian-filesharing-ruling

Obligations on the monitoring software:

1. Connection must be established to an understood peer to peer protocol where a list or peers is retrievable (e.g. an announce for bittorrent protocol).
2. For each entry on the list which a rights holder wishes to pursue, the rights holder (or designate) must establish connection on the port defined by the listed client, and confirm the port responds according to the expected peer to peer protocol.
3. The rights holder or designate must download a minimum of 30% of the work from each peer on the list they wish to pursue. The entire 30% of the work must pass any verification scheme laid out in the protocol (such as passing CRC32 or SHA1 hash checks).
4. Meeting all of the above three points (section 1 to 3) is to be classified as the minimum sufficient proof of an individual infringement on a peer to peer file sharing application. Failure on any of the three requirements disqualifies any action being taken under current or proposed legislation.
5. Chain of custody must be maintained for points 1 to 3 defined as above. Verbose reporting of each step, including start and finishing times, defined to second accuracy and recorded as a UTC timestamp must be associated with each action. All recordings must be made by the system only, with no potential for outside tampering by the rights holder or designate. As such, there must be clear separation between monitoring software manufacturer and software operator.
6. Database entries related to infringement must include at a minimum:
    - Start and finish times for steps 1 to 3 (to second accuracy)
    - IP address identified for infringement
    - Software and protocol implicated in infringement
    - Percentage of file downloaded and verified by the monitoring agency
7. System timing must be maintained in accuracy to within 0.25 seconds. This may be accomplished by NTP synchronisation with a timeserver such as that of NIST (one time server should be defined in the code). Verification must take place on 6 hourly intervals, and time drift inaccuracy recorded and applied as a tolerance in all other time measurements.

2.8.7 Reasons for above list:

1. Required to establish initial lists of internet protocol addresses for which further data should be obtained; those apparently listed to be involved in illicit 'making available' of the work.
2. This step is required to differentiate between announce pollution, as practiced by large trackers such as The Pirate Bay, whereby fake internet protocol addresses, that are not involved in illicit filesharing are fraudulently added to the peering list. Confirming the party responds as expected to all packets ensures that malicious addition of innocent parties does not pollute the infringers list.[12]
3. An offence is only committed under the Copyright, Designs and Patents Act (1988) if a significant portion of the work is copied/made available without permission.[13] We believe a minimum of 30% should be considered a significant portion, and a formal limit will prevent inclusion of individuals who accidentally connect to a torrent swarm then disconnect before sizable transfer of infringing content. Incidental and single packet transfer is simply not enough to meet this obligation.
4. In the absence of any of the three points above the alleged infringement may be insufficient to be considered infringement under the CDPA, or else not have a sufficiently robust basis to successfully identify an account holder.
5. Accurate and precise record keeping is essential to ensure that an individual is identified correctly

[12] http://opentracker.blog.h3q.com/2007/02/12/perfect-deniability/ (as used by The Pirate Bay).
[13] http://www.opsi.gov.uk/acts/acts1988/ukpga_19880048_en_2#pt1-ch2-pb1-l1g16 (Section 3, subsection a).

from the IP address collected as part of steps 1 to 3. A loss of accuracy in this point would preclude incorrect identification due to inaccuracy of records.

6. These requirements alongside 5 provide a robust and clear standard of evidence for supply to the law firm and ultimately the accused individual to support the claim. Absence of this data would be indicative of either poor record keeping or unsatisfactory evidential rigour.
7. The precision of times kept by both data monitor and ISP is essential to ensure correct identification of individuals from the data recorded by both parties. Lax timing in this area will directly lead to false positives in the infringement warning letters due to misidentification of individuals.

2.8.8 Previous monitoring software which has been independently validated by academic investigation has been found wanting. Most worringly, American academics have created an emulator on a commonly used printer which is sufficient to trick monitoring software into adding the printer's IP address to a list of infringers, despite not having the capability to store or transmit the work in question.[14]

2.8.9 All monitoring software used for rights holders to pursue warning letters, disconnection, or legal claims must be independently audited. Auditors must assess evidential rigour, validation protocols undertaken, and chain of custody for evidence collection from point of capture and data verification to subscriber identification. Such audits should be both regular and random, with an average separation of 2 years. No monitoring organisation can be permitted to offer services under the new legislation without this independent authorisation to practice. Such auditing would not prevent independent expert witness analysis should any such case progress to trial. The OFCOM code sets out similar (but less rigorous) requirements by requesting self certification. We strongly believe it must be mandatory for independent scrutiny of all software used.

2.9 *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?*

2.9.1 We believe that the period specified within this paragraph is critically important for the enforcement of illicit filesharing notifications as laid out in the Act. Notably ACS:Law have an average response time from monitoring period to court order of over 5 months (modal and mean averages) in data we have collected from accused individuals.[15] As such, a period such as the aforementioned 10 days is critical in increasing the opportunity for appeals through the use of supporting evidence. Both local router and ISP access logs are ephemeral in nature, issuing CIRs within 10 days would maximise the opportunity for individuals to review access logs for unauthorised access which may have led to the accusation.

2.9.2 We would strongly discourage any attempts by Copyright Holders of their monitoring representatives to force OFCOM to reconsider and lengthen the period from monitoring to letter despatch.

2.10 *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.*

2.10.1 We fully agree with the OFCOM approach to allow invalid CIRs to be discarded by ISPs; it is essential that if measures are set out in code to ensure the robustness and understanding of the CIR to laymen that a consistent and understandable format must be maintained. As such, any CIR which falls outside the guidelines must be ruled invalid and not allowed to be resubmitted at a later point, nor be counted towards the qualification criteria for addition to the list of copyright infringers.

[14] http://dmca.cs.washington.edu/dmca_hotsec08.pdf
[15] Annex 1

2.11 *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.*

2.11.1 Yes, we would broadly agree with the approach similarly to our view of question 4.2. There must be no direct self-certification by ISPs and again there must be the potential for independent evidential auditing. We view it as extremely important that here too transparency is enforced by OFCOM. The process for subscriber identification must be standardised between ISPs as far as possible and the code updated based on the best practices of each service provider. In our view commercial secrecy must not come in the way of potential improvements to the accuracy and robustness of the subscriber identification and therefore all evidence and documents provided to OFCOM must be openly provided online to all.

2.11.2 We believe it abhorrent for any commercial body to pursue secrecy at the cost of higher false positive rates of identification across their industry. As such, we believe OFCOM should encourage and demand a culture of cooperation between ISPs to ensure a consistently accurate approach and sharing of best practices.

2.11.3 It seems necessary to set similar time accuracy requirements on the ISP as those required of the data monitor (see also 2.8.6 (5)). Only with accurate and precise timekeeping are subscriber identifications possible. It should be noted that there can be considerable tolerance in times associated with RADIUS and other leasing protocols in terms of allocation times for IP addresses, indeed RADIUS accounting allows delays as part of the protocol reporting[16]. This must be taken into account in subscriber identification; and as already identified within the draft OFCOM code, identification should not be provided by the ISP if the timestamp of the request falls close to a change in IP lease.

2.12 *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.*

2.12.1 We entirely agree that a time based notification approach is necessary and a fairer approach than a fixed numerical limit. However, we'd argue that it is possible for repeated accidental infringement which may lead to undesirable action against low level infringers. Specifically copyright law can be a confusing area, with different time limits assigned to compositions and performances. For example, a performance of classical music, which is clearly well beyond any life plus seventy year term commonly mentioned in the media with regards to copyright, may be under copyright protection of the orchestra which performed the piece.

2.12.2 It is also questionable as to whether a single instance of infringement is practicable as a limit when applied to multiple occupancy households. Whilst all members of the household should be warned of the consequences and apprised of any warning letter after the first CIR, it may not be clear that more than one member of the household has triggered the CIR. Thus it may be reasonable to consider a higher (but still low) number of CIR reports within a timescale to trigger the next notification event.

2.12.3 We would strongly encourage that all instances of alleged infringement in relation to a single Copyright Owner's CIRs are provided to subscribers and not solely the trigger event for the next letter. This would help to educate multiple occupancy households and those who need to be educated on copyright terms to understand that they are responsible for the infringement and what classifies as such.

[16] http://tools.ietf.org/html/rfc2866#page-12

2.12.4 As such we would suggest the following approach, which we previously submitted to the Department of BIS consultation last year:[17]

a. Send the first letter after two proven infringements are demonstrated for one rights holder with a time separation exceeding one day.
b. The second letter cannot be sent for further instances of infringement noted within one month of the initial letter. After that month has expired, further infringements logged will trigger the second letter after the same requirement of two proven infringements with a time separation exceeding one day.
c. The third letter cannot be sent until two months after the second. Again, no infringements made within those two months may trigger the delivery of the third letter. At the expiry of the two months following delivery of the second letter, ANY further demonstrated instance of infringement will trigger the delivery of the third letter (at this stage, two incidences with a day of separation would not be required).
d. Subsequent letters of warning may be sent at any point after the process has been followed for the initial three warnings. Only once attempts have been made to inform the bill payer of potential hijacking, or legal alternatives, may legal redress be sought. If a period of nine months elapses with no further infringements, the process starts afresh from the first letter.

2.12.5 You will note that our suggestions are close to those proposed by OFCOM with a number of small moderations; a longer cooling off period after the second warning, and a higher trigger number of CIRs for triggering each letter in addition to the time period. As the intent of the Act is to bring about a reduction in illicit filesharing, whilst targeting only the most flagrant and excessive individuals with legal action, we believe our proposals will strike the correct balance of ensuring that small-scale or unintentional infringement is not targeted first. This should ensure that the support of the general public remains with the Copyright Holders' in asserting their legal rights.

2.13 *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?*

2.13.1 We believe there is a necessity to include clear advice on the length of copyright terms. This must include advice on terms for each common type of media (software, music, books and film). It must also include any variable terms dependent on artist/production rights. As mentioned in 2.12.1, copyright can be confusing where there are multiple parties able to assert and invoke different claims in law[18].

2.14 *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.*

2.14.1 We would consider adding the individual to the copyright infringement list immediately after a third strike to be unreasonable. In our proposal (outlined in 2.12.4) the third letter would constitute the final warning. Any subsequent infringement (after a further week from letter dispatch) would then add the individual to the infringer list automatically. We believe due to the first warning being aimed at education, it is likely to take two escalated and strongly worded warnings to discourage infringement. As the primary aim of the legislation is as a deterrent and to reduce levels of infringement, singling out individuals for legal action too early would appear overly strict.

[17] http://beingthreatened.com/resources/Consultation%20Response%20from%20BeingThreatened.pdf
[18] http://www.ipo.gov.uk/types/copy/c-duration/c-duration-faq/c-duration-faq-lasts.htm

2.14.2 We believe that the frequency of requests stated is likely sufficient to identify a large number of infringers and therefore 3 months is an appropriate minimum time before a new list can be requested by copyright owners.

2.15 *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.*

2.15.1 We broadly agree with OFCOM's approach to subscribers appeals. We would be concerned at the punitive nature of charging fees for appeal unless the monetary amount was set at a reachable level for all subscribers. Such a fee may offer a strong disincentive to the government's goals for internet access and broadband reach by discouraging take-up of internet access, or prompting people to cancel their existing accounts.

2.16 *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.*

2.16.1 No view

3 Other Comments

3.1 We wish to again highlight our concern that despite OFCOM's clear wish to set reasonable expectations of the evidential requirements and mandates to correctly identify individuals, there is an extremely high chance that some copyright owners will just ignore the new law and associated guidelines. As there is no compulsion to use the provisions of the Digital Economy Act, some copyright holders who have already found legal threats to be a profitable source of alternative income may persist in generating groundless claims outside the remit of the Act and thus outside the oversight of OFCOM.

3.2 We would strongly encourage OFCOM to use its influence to encourage the government to set out in primary legislation where it is appropriate to use the provisions of the Digital Economy Act and where it is appropriate for a copyright holder to immediately resort to Norwich Pharmacal Orders. Specifically we would strongly encourage that there is a limitation for Norwich Pharmacal Orders in copyright cases that would cause those requested outside the provisions of the Act to be limited to no more than 10 IP addresses in any one order. This would allow copyright owners to pursue those cases so critical as to be requiring action with immediate effect, whilst limiting the current economies of scale leading to repeated spurious actions against innocent individuals (as the economies of scale approach will only then be possible under oversight of the provisions in the code by using the copyright infringement list from the ISP).

3.3 Of concern is the potential that individuals may be held to account for the actions of others. It is notable that a fundamental part of the modern understanding of individual rights is that an individual is not held liable when they have no knowledge or involvement in the actions of another. The account holder cannot and should not be held as having sole responsibility for all acts occurring on their connection. All current wireless security protection is able to be breached in a relatively short time, to hold one individual accountable there must be sufficient proof of their knowledge of, or involvement in, said act.[19]

3.4 It must be mandated that any substantial modification to the OFCOM code following the agreement of a final initial code should be preceded by a consultation, taking a non-partisan approach ensuring that fair representation is given to ISPs, consumer organisations and rights holders. Changes should not be made by OFCOM without such a procedure unless the changes are purely to improve clarity or are cosmetic in basis. If

[19] http://www.opsi.gov.uk/acts/acts1988/ukpga_19880048_en_2#pt1-ch2-pb1-l1g16 (Section 2)

changes are considered to be wide-ranging or substantial in nature a full consultation must be undertaken.

3.5 We strongly believe that the process in entirety must be as open as possible. As such we believe that all reports provided by data monitors on the operation of their systems should be published for public scrutiny. We do not believe that there is any commercial reason to prevent disclosure of this information, as differences between monitors must necessarily affect the data collection. This potentially puts the public at risk from one sub-par monitor. We do not believe that evidential requirements should be set on a free market basis. Without scrutiny, the commercial pressure will be in favour of reduced cost, and increased numbers of infringing IP addresses, leading to reduced accuracy and a significant rise in false positives – the exact opposite of the desired outcome. We also believe that individuals should be able to put questions of published evidence to the data monitors. We envisage that OFCOM would act as arbiter to ensure that only pertinent and well-based questions are passed on to the monitor with a code-defined obligation to answer. Finally, any significant changes to the monitoring code (including a revision history and bug fixes) must be published. This will ensure any quality-affecting flaws in the evidence collecting are appropriately disclosed.

3.6 As part of OFCOM's reporting to the Secretary of State there should be some mention of activities taken in the legal arena outside the remit of the Digital Economy Act which relate to infringement by individual subscribers. This must be provided to assess the efficiency of the act in providing suitable remedy for rights holders. Significant action outside the act would indicate rogue rights holders or insufficient protection or measures within the act which should be addressed.

3.7 We would welcome OFCOM's guidance and clarification on the length of time an IP is held on an infringement list. Once added, would subscribers:

- Remain on the list indefinitely for any future requests from copyright owners
- Be removed from any future list on disclosure of a list containing the subscriber;
  - to be re-added on any subsequent infringement.

  or
  - to be re-added following 3 further warnings.
- Be removed following a fixed time period with no further infringement (i.e. 2 years).

3.8 We would also welcome clarity on the nature of offences necessary to generate warning letters. Presumably the intent is that the notices relate to independent instances of infringement. It is notable that in the code at present it would be possible for 3 tracks on one album to be reported as three infringements separately by the copyright holder at separate dates. This would allow the copyright owner to bypass the time delimited notice periods by artificially creating additional infringements. OFCOM must clarify how this will be avoided in the final draft of the code.

3.9 OFCOM should retain and explicitly state a right to request a freeze on monitoring of UK-based data sets if data monitoring is assessed as insufficiently rigorous. Specifically we believe that it may be possible to set a defined limit in the code for a threshold of false positives or successful appeals necessary to trigger this request. OFCOM must further maintain and publish a list of legitimate and verified data monitors who may provide evidence which reaches the requirements of their code and the Digital Economy Act.

3.10 Before allowing rights holders to establish claim under the act, OFCOM or ISPs should assure themselves of the legitimacy of the copyright owner to claim ownership of the work in question. Sufficient information should be provided as to the transfer of distribution rights or origin of the rights with a company or individual.

3.11 All correspondence under the code must be sent to the subscriber via both email and traditional paper mailing. Most ISPs will list the email address they provide to the subscriber as a contact. This is unlikely to be

the primary email address of most internet subscribers and may not be regularly checked. It is thus essential that a paper copy of correspondence is also provided.

3.12 We would encourage a limit on the number of open cases launched against individuals listed on the copyright infringer list. We are concerned that copyright owners may seek to replicate the monetary success of the 'threatening letter' approach against all subscribers on an infringement list with no actual intent to pursue court action. The courts have so far appeared unwilling to reject court orders to obtain personal details on this basis; therefore the protection against such schemes should be set out in the code.

4 Points of Accuracy

4.1 We note that throughout the consultation document Universal Coordinated Time is referred to as UCT. We believe it worthy of note that the internationally recognised acronym is in fact UTC.[20]

4.2 The proposed FAQ to be included with the letters suggests in point 12 that individuals have a right to obtain personal details from the copyright owner. We believe this data would not be provided due to the exemption provided in Section 35 of the Data Protection Act 1998: *"(2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary - (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)".*[21]

[20] http://en.wikipedia.org/wiki/Coordinated_Universal_Time#Abbreviation
[21] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_5#pt4-l1g35

5 Summary

5.1 We believe that the OFCOM proposals as outlined in the consultation are a step in the right direction. However, we are concerned that there is a lack of detail within some areas, resulting in insufficient specifications to ensure evidence gathered is to a high enough quality and accuracy to be of a legally sound standard.

5.2 While OFCOM's proposals for evidential rigour are similar to our recommendations as outlined in 2.8.6, they lack the depth that is required to reduce the number of false positives, and to prevent abuse of the system. Our proposals attempt to improve that, and we would strongly encourage OFCOM to strengthen and tighten the proposed procedures to match or exceed ours, which be believe are more robust and could be appropriately defended in court if necessary.

5.3 Methods used for gathering evidence by the firms involved in the current filesharing cases have not been published, openly, academically, or as part of publicly available legal hearings, so that only the monitors are aware of the strengths and faults of their data. There has been no independent review process nor is there any disclosure or recourse to individuals before reaching court. We believe it critical for independent and open review to be introduced to the monitoring process, which is best achieved by peer review from open publishing (allowing analysis from lay individuals and academics with an interest) and formal validation before the monitor is allowed to operate under the Act. Significant changes made to the monitoring system would require revalidation to ensure continued accountability. We believe all validation reports, expert witness, audit history/code change reports and other documentation used to establish the strength of evidence should be openly available to all accused under the provisions of the Act and associated code.

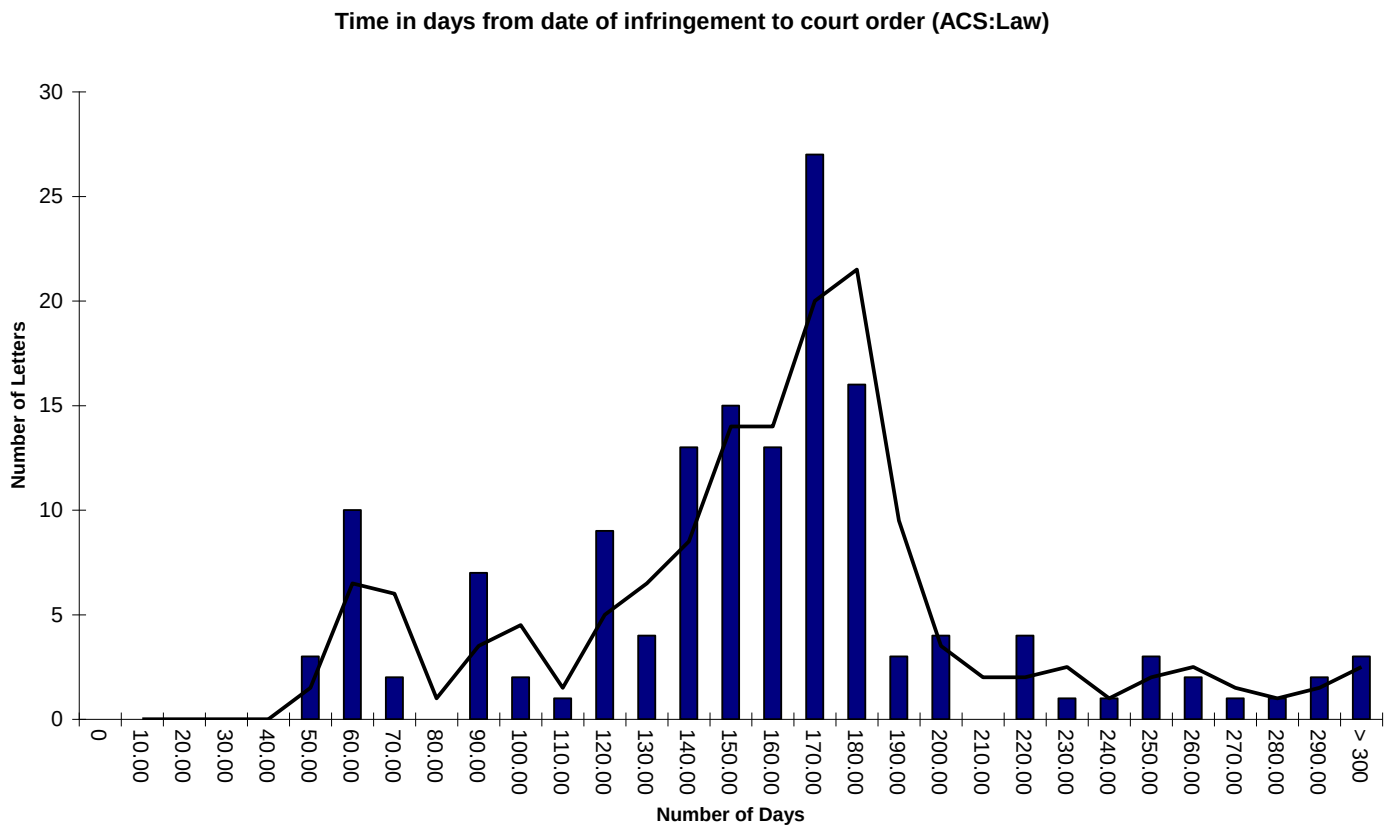
5.4 Whilst not covered in the scope of the consultation, we continue to have concern that some rights holders and law firms have no intention to use the Act even for the most low volume infringement allegations. Within the past month Gallant Macmillan have joined Davenport Lyons and Tilly Bailey and Irvine who have since abandoned their schemes; as well as ACS:Law who are still active in pursuing allegations of illicit file sharing. The action of all four firms, and especially those of Gallant Macmillan and ACS:Law show clear contempt for the Digital Economy Act and no intent to follow the provisions of the Act after enactment. Three of the firms involved have repeatedly refused to disclose any information to establish the strength of the evidence and have not had their evidence tested in court. These scare tactics cause significant distress to many families, many of whom pay up even when they cannot be sure that anyone with authorised access to their Internet connection even committed the offence they were accused of, pushing the number of complaints against ACS:Law with their regulatory body to in excess of 400 individuals.

5.5 Finally, we thank OFCOM for the opportunity to respond to the consultation and look forward to a considered an in depth response which we hope will improve the evidential requirements of the code and take heed of all responses to the consultation.

Annexes

Annex 1: Number of days from alleged infringement to court order.

Annex 1: Number of days from alleged infringement to court order.



Data sourced from individual survey responses to BeingThreatened.com survey. Accuracy of data is limited by any errors in data provided by respondents. Data set for above graph, 147 individuals, responding over 3 months.