RE: Consultation: Online Infringement of Copyright and the Digital Economy Act 2010

FAO Campbell Cowie

Title:

Mr

Forename:

Donald

Surname:

Stone

Representing

Self.

Email:

Ofcom@dontheduck.co.uk

What do you want Ofcom to keep confidential?

Keep part of the response confidential

If you want part of your response kept confidential, which parts?

All email addresses
The name and address of Mr X
The name and address of X
The IP addresses associated with X

If you want part of your response, your name or your organisation to be confidential, 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)?

Yes

I confirm that I have read the declaration

Yes

Ofcom seeks to publish responses on receipt.

Ofcom may publish this response on receipt.

Additional Comments

I have a Masters Degree in Forensic Computing and Security.

I have encountered false accusations being laid against a friend with regards to the illegal sharing of copyrighted content through his internet connection. From my investigations, I have determined that his internet connection could not have been used for this infringement, and that his ISP at the time identified the wrong subscriber to the copyright owner.

With respect to the Digital Economy Act, this could result in an innocent person being punished for the actions of someone not only unknown to them, but unconnected to them in any way other than both being subscribers of the same ISP.

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.**

No comment

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.**

No comment

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?**

No comment

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?**

No comment

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?**

Under section 3.22, any person or organisation providing free Wifi access would become liable for any infringement by third parties. This would include small businesses as well as private individuals. Most people and small businesses would not have the technical knowledge to log which computer or person was connected at a given time, and would therefore be unable to provide details of who may have infringed copyright. Requiring that such people implement a system allowing them to properly process a CIR will overburden them and remove any form of convenience of access to the Wifi network. This will drive away business.

An alternative approach would be to provide a managed gateway product which records IP address assignments to third parties. This would most likely only record the MAC address of the connecting party, which would be insufficient to identify a person. It could be used to indicate which parties were NOT liable, but this would not be conclusive as MAC addresses on network equipment are often programmable. There then arises the question of who would pay for the gateway device.

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?**

Protecting a Wifi access point is something that is fairly simple to achieve. Protecting it effectively, less so.

WEP encrypted Wifi can be 'hacked' trivially. The process of 'hacking' a WEP protected Wifi connection is illegal under the Computer Misuse Act 1990 (unauthorised access), but any subscriber who has this happen to them is likely to be unaware of this until they become the recipient of CIR.

WPA encrypted Wifi is more secure, but the security of WPA is dependant upon the strength of the password. WPA encryption is crackable, but less likely. Should a person receive a CIR, they would naturally assume that the infringement was performed by a legitimate user, rather than an illegitimate one. This would of course once again result in an innocent person being implicated.

The only suggestion I have on this point is the same as for 3.5, a managed gateway device.

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?

I believe that additional information acquired during the discovery phase should be included. In the first legal threats sent out by Davenport Lyons (regarding the game 'Dream Pinball 3D'), the evidence supplied to the accused included the 'hash' value of the shared work, the application being used to infringe the copyright (e-mule, transmission, vuze, etc…) and the username of the person using the application (not always applicable).

It was thanks to this information (the application used to infringe) that I discovered that a friend of mine had been falsely accused. He had never had the application in question on any of his computers, or on any computer connected to his connection.

More recent legal threats (from ACS:LAW) have omitted this information, opting instead to only provide the protocol used to share the infringing content. This leaves any person accused, less informed and less able to determine whether the infringement actually occurred from their connection.

Details of the false accusation are shown in appendix A and proof of innocence is provided in appendix B.

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.**

I believe that although the intentions here are good, it will be subject to abuse. See

"*Challenges and Directions for Monitoring P2P File Sharing Networks ,or, Why My Printer Received a DMCA Takedown Notice*" available at
http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf

One way to stop such abuse would be to require the detection programmes to be open source, therefore subject to independent scrutiny by persons who are affected.

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?**

This would be good from the point of view of the accused. Some log files would retain enough history for them to determine whether a particular computer was even switched on at the time of the infringement. This could allow them to determine the guilty or innocent party.

This measure may be a bit demanding on the copyright owners, as they would need to act quickly and often, rather than saving up a larger list of infringements to deliver in one batch. This could push the costs up for the copyright owners, potentially making the whole CIR process unviable.

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.**

No comment

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.**

Despite the assurance of a witness statement from the ISP that the information they provide is accurate to the best of their knowledge, mistakes are still made. Appendix A shows the legal threat sent to MR X, along with the witness statement from his ISP. In this it clearly states that the protocol used to record IP address assignments uses the unreliable transport protocol UDP.

Appendix B shows the IP address list from a game which Mr X accesses regularly, showing that he did not have the IP address in question.

A fix for this would be to require that ISPs record their IP address assignments using a reliable protocol like TCP/IP, which requires a response confirming receipt of data sent.

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 the situation stands at the moment, and considering my experience with a false accusation being made to a friend of mine, I cannot agree with the proposals as people will be accused, and the burden would then be upon the accused to prove their innocence. This is the wrong way round for a justice based system to work. Obtaining the proof that Mr X was not in possession of the infringing IP address was by no means an easy task. For many people, it would not have been possible, depending upon their circumstances.

When BBC's Watchdog did a report on Davenport Lyons sending out legal threats, there were several people falsely accused. Davenport Lyons released a statement indicating that in the case of Ken and Gill Murdoch of Aberdeen, they were acting in good faith on incorrect information provided by the ISP. Having spoken to them about this, it transpired that they did not even have a wireless connection, nor were they at home (or their computers switched on) at the time of the alleged infringement.

Most people do not have the case dropped against them because they do not have the might of publicity, provided in the Murdoch's case by "Which? Computing" magazine. This leaves them in a position causing a great deal of stress and anxiety. With the CIR scheme, this would mean the potential disconnection of their internet services for something done by another, possibly not even through their internet connection.

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 detailed in the answer to 4.1, additional information gathered at the point of infringement being detected, such as username if applicable, application used for infringement, etc should be provided. This can only serve to help an accused to determine whether it is a computer they are in

control of, or in some cases, whether the CIR is directed at the correct ISP subscriber.

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

No comment

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.**

I disagree with this in principle as it is essentially a case of "you are guilty, now prove that you are innocent". All available evidence thus far would indicate an infringement had occurred from the connection in question. However, this evidence in the first place is flawed.

There is a difficulty here in that there is a difference between civil matters and criminal matters regarding evidence. With this being a civil matter, guilt is determined 'on the balance of probabilities'. There is a lot more weight to the copyright owners evidence (flawed though it may be) than your average person is likely to be able to gather. This puts them in a very weak defensible position, from which they are unlikely to be able to prove their innocence.

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.**

No comment