

Title:

Mr

Forename:

Andrew

Surname:

Hughes

Representing:

Self

Organisation (if applicable):

Email:

ahughes@redhat.com

What do you want Ofcom to keep confidential?:

Keep nothing confidential

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

Ofcom may publish a response summary:

Yes

I confirm that I have read the declaration:

Yes

Ofcom should only publish this response after the consultation has ended:

You may publish my response on receipt

Additional comments:

Question 1: Do you agree that copy management would broaden the range of HD content available on DTT and help secure its long term viability as a platform? :

The BBC's idea that their proposal will broaden the range of HD content on DTT is based on the tentative notion that they will be able to enforce the provision of encryption software on

receivers through the licensing of the Huffman table and that this will then make it more likely that other media companies will provide content for HD DTT. Whether this will actually work in practice is heavily based on how HD DTT takes off, how content providers feel about providing content for it and a lot of luck. It's in now way a given.

What is clear is that imposing this restriction on the service information will make it harder to implement software that decodes, displays and records from HD DTT by requiring this additional licensing step. For one, it actively prevents a Free or Open Source Software (FOSS) implementation from being created as it would require the open publication of the licensed Huffman table. This could cripple the potential adoption of HD DTT by arbitrarily preventing its use in that sector. Many early adopters tend to be enthusiasts who want to work with the new technology and would be prevented from doing so by this need for the BBC's Huffman table.

If HD DTT does not see significant adoption, then it will not receive content from media companies. Market penetration is a much more important factor than the availability of encryption, otherwise content would never have been available on analogue mediums, VHS, SD DTT or the iPlayer, all of which provide unencrypted content. If there is not sufficient market penetration, then the potential availability of encryption is a moot point, and this proposed technique can only work to restrict such penetration.

Question 2: Do you agree that the BBC's proposed multiplex licence amendment represents the most appropriate means for securing an effective content management system on HD DTT? :

The proposed amendment using Huffman encoding is a joke as regards protecting the service information. Those working in the computer security industry would not even see this as a viable encryption technique; it is equivalent to using a Caesar cipher (the encryption used in Roman times) or transmitting the information in morse code. All you need to know is the transformation process which takes the input data and generates the output data, and this can easily be calculated by brute force means.

Not only that, but the service information is only necessary for providing an automated means of decoding the transmission. Anyone interested in copying it can work out manually which video and audio stream makes up BBC 1 for example.

The BBC know this. The Huffman coding idea is the weakest possible form of encrypting the data that will allow them to put themselves in place as gatekeepers over who can use the HD DTT service and will then allow them to impose any requirements they see fit on manufacturers. That's a very dangerous position to put them in.

So no the Huffman coding itself itself is not an effective content management system, and whether it actually works to force manufacturers to include encryption technology remains to be seen.

Question 3: Do you agree with the proposed change to Condition 6 in the Multiplex B Licence? :

No. First and foremost, contrary to what 5.28 says, this will prevent Free or Open Source Software being developed for HD DTT. Doing so would require the illegal publication of the BBC's Huffman table.

The argument in 5.28 that HD Freesat receivers run the open source Linux operating system yet can decode encrypted HD streams is utter nonsense. I would strongly suggest that Ofcom look into the area of FOSS more deeply, starting with the clearer definition of what it is from <http://www.gnu.org/philosophy/free-sw.html> , before accepting such a pathetic argument. Just because a receiver runs a FOSS operating system does not mean that it can't include proprietary software that implements closed techniques such as Freesat encryption or the Huffman coding technique proposed by the BBC.

The true issue is that you can't produce FOSS software which decodes the stream, as it would require the source code to include the BBC's Huffman table. Publishing that would be illegal.

Question 4: Do you agree that Multiplexes C and D should be granted a similar amendment to their Licences as Multiplex B?. :

No, though this raises different issues as these are not provided by a publicly funded broadcaster. A more viable option, though one I dislike, would be for these to be properly encrypted by the commercial companies who use them.

Question 5: Do you agree that the BBC's proposed approach for implementing content management would safeguard citizens and consumers legitimate use of HD content, and if not, what additional guarantees would be appropriate? :

The question itself here is nonsense; why would consumers and citizens need their use of HD content to be legitimate? I expect they would think turning on their television set is a perfectly legitimate action and most would be unaware of any of the technology used to provide the HD DTT service. Generally, such content management techniques prove to be breakable by those who wish to illegally copy and distribute the media, while being intrusive towards the general public's legitimate use of the data.

The BBC's proposal would effect consumers in limiting their choice of available ways of receiving the service. One viable way of receiving SD DTT at present is to use a USB stick in a computer. The BBC's proposal would require software for these devices to use the Huffman table. As stated in the response to question 3, Free or Open Source Software implementations of this, as are currently abundant for SD transmissions, would be illegal.

Question 6: Do you agree that the BBC's proposed choice of content management technologies will have only a negligible impact on the cost of HD DTT receivers and their interoperability with other HD consumer equipment? .. :

No, I disagree. It will prevent the development of FOSS decoders and their use on receivers, requiring manufacturers to license or develop a proprietary implementation which can not be shared with others. It will also prevent the use of FOSS implementations on computers from using the DTT transmissions. See question 3 & 5 on this matter.

Question 7: Do stakeholders agree that the BBC's proposed Huffman Code licensing arrangements would have a negligible effect on the market for HD DTT receivers? :

Yes, the Huffman code licensing would have a significant negligible effect, placing the BBC as a gatekeeper over receiver development and making the development of FOSS support for HD DTT illegal.

Question 8: Do the BBC's proposed content management states and their permitted use for different categories of HD content meet the requirements of other HD broadcasters on DTT? . :

I don't know what these requirements are. Attempts at 'content management', the process of restricting the use of media at the copyright holders' discretion, often beyond the remit of copyright protection, have proven breakable and only hurt legitimate users. I don't see any benefit in providing it for either media companies or consumers, but many downsides.

Question 9: Are there any issues that you consider Ofcom should take into account in assessing the BBC's proposal, that have not been addressed by this consultation?:

No, but the issue of Free and Open Source Software needs to be much more carefully considered, rather than dismissed by the irrelevant argument used in 5.28.