Prometheus
Vol. 28, No. 4, December 2010, 395–399

Routledge
Taylor & Francis Group

RESPONSE

Response to paper by Birgitte Andersen on the Digital Economy Act

Andrew Heaney*

TalkTalk Telecom Group PLC, London, UK

Andrew Heaney has been executive director of strategy and regulation with TalkTalk since 2007. He was previously a competition policy director with Ofcom and a partner with Spectrum Strategy Consultants.

Introduction

Birgitte Andersen's Proposition paper highlights many of the shortcomings of the government's approach to tackling illegal file sharing expressed in the Digital Economy Act (DEA). Andersen describes the overall impact of their approach as 'less for everyone', outlining in particular the negative effects of reduced exposure of content and restrictions on legitimate use of the Internet.

I take a slightly different perspective – I work for TalkTalk (the UK's second largest Internet service provider (ISP)) and we think about things from the perspective of our customers and providing them with Internet access.[1] However, I come to a similar but more stark conclusion – the government's approach will do little to help rights holders and will be highly harmful in the process. My simple view of whether the government's planned measures are a good idea is based on an assessment of three things:

- How much benefit will it deliver (A)?
- Will it cause harmful collateral damage (B)?
- How much will it cost to implement/operate (C)?

In mathematical terms the measures would be a good thing if (an economist might call this a cost–benefit analysis, a lawyer might call it a proportionality test):

$$A > B + C$$

… or preferably (if we are to apply the current government's desire to reduce burdens on individuals and businesses):

$$A >> B + C$$

Unfortunately, the government's measures do not pass this simple but critical test: the benefits will be small, and yet the implementation costs and harm will be substantial, far outweighing the benefits. I expand on these points below. Before looking at

*Email: andrew.heaney@talktalkgroup.com

ISSN 0810-9028 print/ISSN 1470-1030 online

DOI: 10.1080/08109028.2010.537184
http://www.informaworld.com

each of these points, it is worth understanding what was proposed and particularly the approach to detecting illegal file sharers.

The flaw in the detection system

The approach laid out in the DEA will mean that subscribers of connections that are used for illegal file sharing (using 'peer-to-peer' or P2P technology) first receive warning letters. If their connection is repeatedly used[2] for illegal file sharing they will be placed on an 'offenders register' of individuals who can be targeted for court action under existing copyright law (the rights holders decide whether to pursue such court action). The DEA also allows for the possibility of further legislation to require ISPs to disconnect subscribers whose connections are repeatedly used for illegal file sharing (rights holders are lobbying hard for this extension).

Critically, this approach does not, in fact, detect the individual infringer. The detection method that is used is based on identifying the IP address of the connection the infringer is using.[3] That IP address is sent to the ISP and the ISP can identify the subscriber of the connection. It is the subscriber who will be sent the warning letters, put on the offenders' register, prosecuted in court and/or disconnected.

Yet the likelihood is that the actual infringer is not the subscriber – most connections are shared between several people in the household (and can also be used by wi-fi hackers). This mismatch between subscriber and infringer will be particularly high in this context since file sharers tend to be young and likely to use the broadband connection of a parent or to live in shared accommodation. We estimate that perhaps two in every three subscribers accused will not be the infringer and so will be innocent.

Thus, using the government's approach, the subscriber will in effect be deemed to be liable for the behaviour of third parties. Such a construct is unfair and also inconsistent with law – a third party is only responsible for copyright infringement by another person if they 'authorised' infringement by that person. Allowing, for instance, a son or daughter to use an Internet connection is not authorising them to file share illegally. Such an approach effectively places the subscriber in the position of policeman of the connection.

This flaw in the detection system weakens the case for introducing the measures – it reduces the benefit (since actual infringers know they cannot be accurately detected), it will cause harm (since many innocent people will be falsely accused) and it adds operating costs (since it will be necessary to have many appeals against these false accusations).

How significant are the benefits?

The content industries (particularly music and film) frequently tout figures of hundreds of millions of pounds in revenue that are lost each year because of illegal file sharing, suggesting that this is the prize that will result from tackling illegal file sharing (as Andersen points out, these figures have little sound evidence underpinning them). Of course, the relevant figure is not what has been lost, but rather what can be regained as a result of introducing these particular measures.

The reality today is that you cannot stop consumers from illegally copying copyrighted material. It is now almost costless to make a perfect copy of a music track or film. And it can be done without risk of detection. Though the detection method proposed in the DEA will detect (albeit inaccurately) file sharing by means of P2P

technology, there are several other techniques that individuals can use to get their content for free if they wish to avoid detection. Some of the examples are:

- using a proxy server so that the IP address is that of a server in (say) Mongolia;
- recording from a radio streaming service (akin to recording from the Top40 on a Sunday evening onto a cassette tape);
- using a so-called 'cyber-locker';
- using a Usenet service;
- hacking into a neighbour's wi-fi network or using a open wi-fi network; or
- using an overseas pay site (at a fraction of the price of UK services).

In fact, in the last two years over half of illegal file sharing has shifted to these other methods. Thus, trying to stop illegal file sharing by tackling P2P file sharing is likely to be about as successful as King Canute was at halting the incoming tide – the bald truth is that trying to stop illegal file sharing using deterrent measures will be futile. Given this reality, we estimate that, at best, the measures might result in an extra £10m or £20m of revenue for the content industries.

What collateral damage will it cause?

Andersen identifies some of the downsides that would result, such as preventing legitimate and beneficial Internet use. There are, in fact, many many other harmful side effects. The most significant is that millions of innocent subscribers who have not infringed themselves will be sent warning letters, put on the offenders' register, targeted for prosecution in court or disconnected. Their only recourse to stop this happening will be to appeal against the action. However, the (previous) government decided on an approach to 'appeals' whereby (in a reversal of the normal presumption of innocence) accused subscribers would be deemed 'guilty' (and lose their appeal) unless they could demonstrate that they had not carried out the illegal file sharing, and prove they had secured their network connection against hackers.[4] Given the millions of subscribers likely to be sent letters,[5] this approach will result in vast numbers of innocent subscribers being wrongfully pursued and possibly wrongfully disconnected.

These unfounded accusations may lead to subscribers having to take steps to secure their home networks against use by hackers. This could, in some cases, cost subscribers over £100 since they would need to upgrade to a more modern encryption technique, such as WPA2. This will require them to replace equipment that is incompatible with WPA2, such as certain modems and games consoles. Across the UK, we think the cost of this forced upgrade might be £30m per year.

Another major negative impact will be on open wi-fi networks, such as those offered in coffee shops, libraries and hotels – these operators may close or restrict their services as a result of the measures. The legislation has not exempted these networks (if they were exempted, it would leave another easy route for individuals to file share undetected). Instead, under the legislation many of these networks will be expected to log subscribers' details and/or take actions to prevent illegal file sharing. This will undoubtedly add cost, which in many cases may lead to the network closing. The risk of court action or disconnection might also cause them to close their networks.

It is highly likely that some subscribers who receive warning letters will (to 'wipe their slate clean') move to another ISP. This will result in significant churn and

migration costs. This impact will be greater if, as proposed by Ofcom in its code,[6] most smaller ISPs will be exempted from the code and so will attract those wishing to avoid being detected.[7] Of course this difference in treatment among ISPs will also result in a competitive distortion.

One of the most evident downsides of the measures is the harm caused by subscribers being disconnected after repeated infringements on their connection. Obviously this will be grossly unwarranted and unfair to the many subscribers who will have done nothing wrong or illegal themselves (since the infringement was by another user of the connection). There may be hundreds of thousands of innocent subscribers who could be disconnected in this way.

Even for a subscriber who has actually illegally file shared (i.e. they were the infringer), such a 'punishment' would have a drastic effect and would probably be disproportionate (given the magnitude of the 'crime'). The subscriber would be deprived of key rights and capabilities such as freedom of expression and the ability to use the Internet for key tasks, such as communication, study, e-government and commerce. Unlike in a court situation, there is no attempt to assess the proportionality of the punishment, but rather there is a one-size-fits-all punishment that is applied irrespective of circumstances. Worse still, in a form of medieval 'collective punishment', all the other users of the connection will also be deprived of these rights and abilities. In an age when we are trying to encourage Internet use, such an approach beggars belief.

I could go on and describe other downsides (or add further support to the ones Andersen highlights, such as deterring experimentation and innovation), but I hope the picture is clear: the measures the DEA imposes will cause clear and severe harm. In addition, the whole system will be costly to implement. Over six million individuals illegally file share today. Implementing, operating and administering the systems and processes to identify infringement, match IP addresses to subscribers, send letters to the subscribers, manage calls from concerned customers and handle appeals involving hundreds of ISPs and rights holders and millions of customers is a complex and substantial undertaking. Having looked at some of the issues it raises, we estimate the total overall cost will be over £50m per year.

Conclusion

We see the illogic behind the DEA as very clear. The measures will be expensive to implement, will deliver minimal benefit to rights holders, and yet will cause massive harm to citizens and Internet usage across the UK. In other words, $A << B + C$. It is difficult to conceive of a more hopeless set of measures. Which, of course, begs the question: what should be done? This question must be answered from the perspective of a world in which copying is easy and it is mostly futile to try and stop illegal file sharing. Illegal file sharing will continue whatever deterrent measures are put in place (even if the Internet were shut down, kids would swap memory sticks in the playground). Stopping illegal file sharing is a unwinnable battle.

The creative industries have to adapt to this new reality rather than, in Canute fashion, defend the old. This might mean in some cases that certain business models are no longer viable. There will probably be more focus on new revenue sources, such as more live concerts, merchandising or 3D cinema (and less on selling copyrighted music tracks or DVDs). Alongside there must be a focus on carrots to make people want to pay for content (even though they can avoid paying if they want to). These

should include educating people about the impacts of not paying (in effect trying to make illegal file sharing socially unacceptable) and creating attractive services to entice users back. Unfortunately, the DEA has done nothing to help this happen.

Trying to stop illegal file sharing in the way the government has proposed will be futile and damaging.

A footnote

I work for TalkTalk and have led TalkTalk's efforts to try and prevent the government's proposals being introduced. We won some battles (believe me, some of the proposals were even worse than those that got through), but lost others (since, as you can see, what has become legislation is absurd). However, our fight is not over – we have applied (with BT) for the legislation to be judicially reviewed and the hearing will be early next year. You can read our case (though I warn that it is rather legalistic).[8]

Notes

1. I should say that my opinions, though coloured by TalkTalk, are very much my own. I should also mention, on behalf of TalkTalk, that TalkTalk does not encourage, condone or induce illegal file sharing. TalkTalk accepts that rights holders have legitimate intellectual property rights and is willing to work with rights holders to address the impacts of illegal file sharing. However, TalkTalk will fight vigorously against measures that are unjustified and harmful to its customers.
2. According to Ofcom's draft code of practice for the operation of the legislation, a connection will be considered as being repeatedly used if it is used for illegal file sharing in more than three separate 30 day periods in a 12-month period.
3. This is done by the rights holder participating in a 'P2P torrent', which is effectively a community of filesharers. Participants expose their IP address.
4. Notably, if these subscribers are prosecuted in court, they will probably be found innocent since courts work on the basis that individuals will be found guilty only if it is established that they actually infringed copyright themselves. A court is unlikely, we think, to see infringement on the connection as sufficient evidence to prove infringement by the individual.
5. There are an estimated six million illegal file sharers in the UK.
6. Ofcom is responsible for developing the code of practice as to how the legislation will work in practice.
7. Both subscribers who are infringers and subscribers who are not infringers will wish to avoid detection.
8. See http://www.talktalkblog.co.uk/download/sfg-final.pdf.