DIGITAL ECONOMY BILL

ONLINE INFRINGEMENT OF COPYRIGHT:
LIBRARIES, UNIVERSITIES AND WI-FI PROVIDERS

FEBRUARY 2010

Summary

Libraries and Universities (and other wi-fi providers) offer internet access via a number of different routes, fixed and wireless, and through a number of different models including staff, subscriber, student and free access.

The question of whether a university, library or wi-fi provider is an ISP[1] or subscriber in terms of the Bill is a critical one and we have attempted to summarise the different positions and the implications below:

Where the University/library/wi-fi provider is an ISP

If falling into the ISP definition, an establishment will have to comply with the obligations falling upon ISPs[2], provided the level of infringement on their network was such as to breach any threshold limit set out in the code.

Where the University/library/wi-fi provider is a subscriber

If falling into the subscriber category, an establishment could receive notification notices from their ISP where their connection was linked to an allegation of copyright infringement. It would be up to the establishment to take action if they wished to avoid receiving further letters or avoid the prospect of inclusion on a copyright infringement list. ISPs will be required to provide information about the sort of action that could be taken to try and prevent further infringement. In the event of the establishment seeking to appeal against a letter or being placed on a list, it would be for the appeals body to make a judgement on each individual case in the light of individual circumstances.

Our intention is that the code should require ISPs to provide generic advice and information on how to tackle infringement as well as how to protect a wireless connection/network and that such advice is appropriate for the type of establishment in question. We will add a requirement in the Bill under clause 8 that this is a provision that the code must include.

Libraries

At present, the majority of current access to the internet provided (to the public) in libraries is via fixed library terminals. The speed of access varies greatly, but on average is about 1 Mb/sec. Users usually book-in for a set period of time.

Current levels of use

A report into the role of libraries in supporting and promoting digital inclusion (MLA January 2010) found high levels of library visits to use the internet connections on offer. Typically, there are between 1,500 (small libraries) and 6,500 (large libraries) visits per library per week specifically to use the internet.

Current restrictions on use

[1] Internet Service Provider

[2] The obligations are to send notification letters and facilitate copyright owners' legal action. See clauses 4(4) and 5(1) of the Digital Economy Bill

There is no standard set of conditions or restrictions but the following represents what is generally implemented:

- No downloads on to library computer desktops (although downloads onto mobile technology are generally permitted)
- Library services are able to pinpoint specific downloads to time and terminal (where fixed) after the fact. It could possibly be used to block library users, although libraries are concerned how this would in practice operate. This would raise resource issues as it would require additional staff to monitor traffic and downloads and ensure filters are regularly refreshed;
- Firewalls do not allow access to a number of sites, such as those containing Flash technology (these firewalls are generally for security rather than file-sharing reasons);
- Libraries will have a filter system, which should block access to known unlawful sites – although it is difficult to update filters often enough to keep up with new file sharing sites; and
- Acceptable conditions of use policy – all library services should have a "conditions of use" policy, which users have to agree to before getting access to the network, for example no unlawful activity including copyright infringement is permitted. The policy usually stipulates that legal liability for unlawful activities sits with the individual not the library service

Where access is via a library fixed terminal the key factor is that library machines do not have P2P[3] software and are set up to block attempted downloads and installation of the software. For fixed library terminals it is unlikely therefore they can – or could - be used for copyright infringement via P2P networks.

Case study - Westminster

Westminster libraries provide an example of the type of action that libraries take. Users book in to use a PC for a particular period. They are registered to allow the library to distinguish between different user groups – children, adult, student etc. They use "Websense" to filter traffic on their fixed network. This allows them to ensure that different user groups can access different types of sites – for example ensuring that children using their facilities cannot access adult sites. It also blocks the use of P2P technology.

In the case of Westminster, their central location and proximity to mainline rail connections means a large proportion of users are transient and only use the facilities to check e-mails.

Wireless access in libraries

Some libraries offer wireless access and most refurbishments and new library buildings include wi-fi access. The Museums, Libraries and Archives Council (MLA) have recently negotiated for public libraries to connect to the JANET network (see universities note below) which will facilitate many more libraries being able to offer more wi-fi access in the near future. There are measures that can be placed on wireless networks to either restrict

[3] P2P – peer to peer file sharing. In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

access to sites or restrict use of certain technologies or protocols (for example routing all traffic through a proxy server which did not support the use of particular technologies).

Exemption for libraries?

We have considered the extent to which an exemption might be provided in the legislation. We cannot give blanket exemptions for any such establishment. This would send entirely the wrong signal and could lead to “fake” organisations being set up, claiming an exemption and becoming a hub for copyright infringement. Similarly existing establishments might simply ignore the issue of copyright infringement (or treat as “too difficult”) and allow users to infringe copyright with effective immunity.

However, these establishments do face particular challenges in tackling copyright infringement. A sensible way forward would be for ISPs to provide generic information about how to secure wireless connections or install the type of privacy controls that can impose restrictions on those seeking to infringe copyright. This advice should be appropriate for the type and size of the establishment. In the event of an infringement occurring and being linked to the establishment in question, it would be for the appeals body to make a judgement on each individual case in the light of individual circumstances. **We will add a requirement in the Bill under clause 8 that the code <u>must</u> include a requirement that ISPs provide appropriate advice.** Also there is scope for the code to reflect the position of librarires, universities or wi-fi providers. For example. there may be a case for such institutions to have differing sets of thresholds which trigger notification letters. This would be a matter for the code and we would urge the relevant representative bodies to consider now how bets to engage in the code development process.

Universities

The position as regards universities is far more complex. Many universities have had their networks established for considerable periods of time and pre-date the internet. Most have their own IP[4] allocation. In addition they can provide network facilities for nearby research, medical and FE/HE (Further Education/Higher Education) establishments and business/commercial concerns.

Some universities manage their networks across the whole of their estate (ie faculties and halls of residence); others contract out coverage in halls to third party suppliers.

P2P file-sharing is used, sometimes heavily. This is not surprising, given the original impetus behind P2P development was to allow research establishments to share large volumes of data effectively. Anecdotally, we understand that a fairly typical university currently receives between one complaint a week to one a day from copyright owners.

JANET (UK) is the not-for-profit organisation which provides the backbone network that connects universities, colleges and schools to each other and to the internet on behalf of the Joint Information Systems Committee (JISC). In some instances, JANET is responsible for IP address allocation.

The relationship between universities and JANET is complex, depends on a number of different variables and there is no one standard model. In some cases it might be that JANET is acting as ISP with the university as a subscriber; in most cases though JANET is acting more as a communications provider and the university itself might be regarded as the ISP. Without examining the situation for each university and their relationship with JANET, it is not possible to say whether JANET is acting as an ISP or not; nor is it clear

[4] The Internet Protocol (IP) address is the identifier which allows one node (e.g. user, PC, website etc) on the internet to find another. IP addresses are allocated internationally. Usually an ISP will have a block of IP addresses which it continually allocates and reallocates to subscribers. Some universities have their own IP allocation; JANET also has an allocation.

whether a university is a subscriber, ISP or is simply not in the scope of the Bill. As such, we cannot say simply who the ISP is and who is the subscriber, only that this is something that each university would have to look at and establish for themselves.

Thus far, this has not been an issue. We understand that so far as current enforcement action is concerned, the Federation Against Copyright Theft (FACT) takes a pragmatic view and sends any infringement notice to the organisation to which the IP address was allocated. In some instances this might be JANET, in others the notice would go direct to the university. The information on which organisation has which IP address allocated to it is freely and publically available.

Case study – Imperial College, London

Imperial College, London covers 12,000 students in 6 campuses, 6,000 staff plus neighbouring medical and research facilities, the Royal Society and the Royal Geographical Society. They estimate there are between 40-45,000 units connected on their network. The bandwidth is very high (many universities have connections from 1 to 10Gbps).

For staff and students they provide access both in the University itself but also in halls of residence or in wireless areas. Access is closed but the bandwidth and cap is typically quite high. Most of the network is closed with connections going to other associated educational and research establishments (which can be overseas), although they can link to the internet itself.

Action on copyright infringement

JANET already takes a strong stance on copyright infringement. JANET has a strict acceptable use policy which does not allow the network to be used for copyright infringement and requires all user organisations to have a similar policy. Any organisation connected to JANET which breaches this policy and does not take action to address this would be reported to JISC in the first instance, and face their connection being withdrawn if the activity continued.

Some Universities take an extremely strict line. Imperial College takes the following action where a student is identified in connection with a breach of the acceptable use policy. The first occasion merits a 24 hour account suspension. If repeated, the account would be suspended again but for a longer period. Any further breach would lead to disciplinary action against the student. Where staff are involved, the measures are more severe with a second breach leading to disciplinary action; this usually results in dismissal.

However, it does not seem that the practice at Imperial College is common across all universities and represents the high point of action against infringement.

Rather, the picture that emerges is a mixed one. It is clear that JANET and some universities already take far stricter action on copyright infringement than is being proposed in the Bill. For others, a baseline set of obligations and actions might support them in tackling online infringement of copyright.

It does not seem sensible to force those universities who already have a system providing very effective action against copyright infringement to abandon it and replace it with an alternative.

However, the Government does not consider that it would be appropriate to create a simple exemption for universities, other FE/HE establishments – or indeed for libraries. We expect for those establishments where effective action is already being taken, that it makes sense for all parties to continue with existing arrangements. For others, the provision of generic advice should allow them to consider what steps they might take and for any appeals to be considered by the independent body on a case by case basis.

Wi-fi networks

There is an increasing variety of wi-fi networks offering internet access. These range from small premise-restricted networks in coffee shops or pubs, hotels and conference centres to open access networks covering urban areas or holiday parks. The connections offered reflect this variety from the limited bandwidth and capacity of a coffee shop up to high speed connections in business hotels. They are either available at no charge – provided by the local authority or as part of a wider commercial package, eg included in the cost of refreshments or hotel accommodation. Some are commercial products seeking to compete with the fixed and mobile networks.

Depending on the type of service and the nature of their relationship with their consumers, a wi-fi provider may be an ISP or a subscriber. In some circumstances they might be regarded as a communications provider (if so they would need to comply with the General Conditions set out under the Communications Act 2003).

Case study - urban wi-fi: Swindon

Swindon Borough Council is offering a free wi-fi service providing internet access to residents. The service is provided by a commercial partnership between the local council and a private sector company (with the council taking a minority 35% share) and is expected to operate at a profit. It launched in December 2009.

Currently the Swindon wi-fi network is offering a two tier service. The first is a free basic service which offers users access to e-mail and web browsing.

The second is a subscription 20Mb/s service at £10 per month (currently under trial). Subscribers who wish to use the service in the home or office are advised to install a signal booster. This suggests the service is designed more for nomadic occasional use and therefore may not lend itself to the large levels of data transfer typical of significant levels of infringement.

The type of free or “coffee shop” access is a basic bandwidth service which offers users access to e-mail and web browsing. It is seems unlikely that the type of free broadband service currently available would be sufficient to support any file-sharing or could be used for significant copyright infringement. Under our proposals such a service is more likely to receive notification letters as a subscriber than as an ISP. As before there are measures that can be taken to reduce the possibility of infringement with any cases on appeal being considered on their merits.

In contrast, the broadband rates one might expect of a commercially offered wi-fi service in competition with the fixed and mobile providers would almost certainly be sufficient to support file-sharing. If in scope, the wi-fi provider would have to comply with the initial obligations, as would any other ISP.

Hotels, holiday parks and conference centres will in many cases offer a level of service where infringement could become a significant problem. Business users will want a high speed bandwidth connection and wireless internet access is becoming a default requirement for holiday parks and the like. Each establishment would need to examine their position and decide whether they were a subscriber, ISP or indeed communications provider in terms of the Bill, although it appears unlikely that few other than possibly the large hotel chains or conference centres might be ISPs. Again, advice should be made available which is relevant and proportionate to the establishment.

TOP-LEVEL GUIDE: INFORMATION AND MEASURES TO TACKLE ON-LINE INFRINGEMENT

There is any number of technical solutions to tackle infringement (and other forms of unlawful, undesirable or illegal internet activity). These range from the simple and cheap to the complex and expensive. We assume that the larger networks will have some degree of technical expertise available to them (either in house or via contract). This note is aimed at the small or community networks. No solution is 100% effective; rather the aim should be to ensure that anyone who wishes to misuse the connection to infringe copyright would need to make a conscious decision and effort to do so.

Not all measures are technical. There are non-technical measures which can go some way to deterring unlawful activity.

Where practicable, users should have to agree an “acceptable use policy”. All ISPs have such a policy as do all libraries and universities. This in itself will not stop people infringing but it will make them aware of the legal position. As many people genuinely are not aware that file-sharing material like music or films is unlawful, highlighting this in a policy could deter some.

Small wi-fi providers based in the community (eg local pubs, churches, community halls) might consider requiring users to register (ie so that only those registered could use a secure network). This would prevent transient access and make it easier to police the network through social pressure.

The type of simple measures which can tackle infringement include:

- Blocking any software or application downloads onto fixed computer desktops
- Enabling the privacy/security features of the router, if these are available.
- Installing Firewalls that do not allow access to a number of sites, such as those containing Flash technology
- Filters to block various sites
- Acceptable conditions of use policy – a “conditions of use” policy, which users have to agree to before getting access to the network, for example no unlawful activity including copyright infringement is permitted.

These will not prevent an individual from infringing copyright but should ensure they will have to make a conscious decision to work around the measures and will need a degree of technical knowledge.

The ISP providing the connection can provide advice on how to secure and protect a connection or network. They also offer some privacy and parental controls, either as part of a package or a low cost add-on.

Wireless connections are harder to secure. It is straightforward to limit use to only authorised users – via a password or by registering the PCs that can access. Access might also be limited to particular times of the day. Preventing authorised users from miss-using a connection is more difficult. One option is to route all traffic via a proxy server which does not support or allow (eg) use of file-sharing technologies. Another is to place similar restrictions on the router.

The “Get Safe Online” website (http://www.getsafeonline.org/) – supported by HMG and Ofcom – lists three companies who provide filters and software which can block or filter content and who can also block the use of P2P programmes: Cybersitter, Net Nanny, and Cyberpatrol.

It also provides a link through to other sites such as GetNetWise.org which lists and evaluates a wider range of products including BSafe, Safe Eyes, ChildSafe and Cybersentinel.

These products typically cost in the region of US$40 (about £30) and allow the user to block the most popular P2P applications such as: Bit Torrent, eMule, Gnutella, Kazaa, Morpheus, and Limewire.

http://www.bis.gov.uk/digitaleconomybill/

First published February 2010. Crown Copyright. URN 10/745

BIS Department for Business Innovation & Skills

INTELLECTUAL PROPERTY OFFICE

dcms department for culture, media and sport