2010 - EC consultation on the implementation of the Directive on Electronic Commerce

This is JANET(UK)'s response to the European Commission's consultation "on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic Commerce (2000/31/EC)" [1]. JANET(UK) is the operator of JANET, the UK's National Research and Education Network (NREN) which connects universities, colleges, research organisations and regional schools networks in the UK together, to the public Internet and to peer NRENs in other European countries through the GEANT network. Although JANET is a private network, the Directive's provisions are relevant to us and the organisations we connect in our roles as network providers. This response therefore covers those parts of the consultation relevant to Internet Service Providers, specifically questions 52 to 69.

52. Overall, have you had any difficulties with the interpretation of the provisions on the liability of the intermediary service providers? If so, which?
Yes. Many education organisations and networks wish to block access to particular Internet locations or protocols that are inappropriate for their users or that present a threat to the security of their computers or networks; alternatively they may wish to replace potentially harmful content with a warning. Concern has been expressed that it this might fall foul of Article 12(1)(c)'s test that the service provider "does not select or modify the information contained in the transmission", since it might be seen as performing such selection or modification. As in our response to question 58 below, there are increasing expectations by users, Government and others that networks and organisations will use filtering and blocking to deal with many types of inappropriate network use, thereby making networks safer for electronic commerce. Clarity that such activities do not risk the provider's 'mere conduit' status is therefore increasingly important.
These concerns are increased because it is not clear whether a provider using blocking or filtering risks losing all 'mere conduit' protection from liability, or only in respect of those communications that were filtered. If an organisation that filtered some inappropriate e-mails to protect its users might thereby become liable for all copyright breaches taking place on its network, this could strongly discourage the adoption of filtering.
We therefore believe that at least clarification, and possibly strengthening, of these liability protections is necessary if intermediaries are to fulfil the expectations of their customers and governments to provide systems that can support the further development of e-Commerce.
53. Have you had any difficulties with the interpretation of the term "actual knowledge" in Articles 13(1)(e) and 14(1)(a) with respect to the removal of problematic information? Are you aware of any situations where this criterion has proved counter-productive for providers voluntarily making efforts to detect illegal activities?
Yes. As with Article 12(1) discussed above, Article 14(1)(a) has caused concerns that an organisation that attempts to proactively check for inappropriate material uploaded by others may acquire "actual knowledge" of unlawful material and thereby lose protection from liability (An article by Out-law [2] highlights the varying national positions on this question). It appears

counter-productive that the current law encourages hosting services that want legal certainty to do nothing proactive, but wait until a third party informs them of inappropriate or unlawful material, thus increasing the period for which it is available.
For hosting sites there is also a problem that checking for one type of inappropriate use might result in liability for all types of legal infringement. As the Commission study [3] notes on page 14, an organisation might well have the human or technical ability to identify material inappropriate for children but not have the skills necessary to determine whether material may be hosted in breach of copyright. Again, current law could be read as requiring competence in identifying every kind of inappropriate use before proactively searching for any one kind.

54. Have you had any difficulties with the interpretation of the term "expeditious" in Articles 13(1)(e) and 14(1)(b) with respect to the removal of problematic information?

No. Since a wide range of circumstances might legitimately affect the speed with which an organisation removes problematic information, we consider that it is better to allow courts to determine in each case whether or not the time taken was reasonable, rather than imposing a fixed limit that would inevitably be inappropriate for some circumstances. For example UK universities and colleges have a legal duty to promote free speech under section 43 of the *Education (No.2) Act 1986* [4], which may require them to take additional legal advice before removing material, or otherwise follow a different removal process to a commercial hosting service. We consider, however, that it is unlikely that any circumstances would require a faster response than the two calendar days required by the UK's *Terrorism Act 2006* [5].

55. Are you aware of any notice and take-down procedures, as mentioned in Article 14.1(b) of the Directive, being defined by national law?

Sections 3&4 of the *UK Terrorism Act 2006* [5] require an organisation to remove or modify within two working days any electronically published statement if they are informed by a police constable that it is unlawfully terrorism-related. If they do not do so then they are held to have approved the publication of the statement, potentially a serious criminal offence.

56. What practical experience do you have regarding the procedures for notice and take-down? Have they worked correctly? If not, why not, in your view?

The Law Commission's 2002 report Defamation and the Internet: A Preliminary Investigation [6]concluded of that notice and takedown regime:

"There is a strong case for reviewing the way that defamation law impacts on internet service providers. While actions against primary publishers are usually decided on their merits, the current law places secondary publishers under some pressure to remove material without considering whether it is in the public interest, or whether it is true. These pressures appear to bear particularly harshly on ISPs, whom claimants often see as "tactical targets". There is a possible conflict between the pressure to remove material, even if true, and the emphasis placed upon freedom of expression under the European Convention of Human Rights. Although it is a legitimate goal of the law to protect the reputation of others, it is important to ask whether this goal can be achieved through other means."

Although the majority of takedown notices under all notice and take-down regimes appear well-founded we have also experienced notices that, as the Law Commission feared, were not. In one case a business supplying to the university sector appeared to be trying to use take-down notices to disadvantage its competitors. Since universities and colleges have a legal duty to ensure that freedom of speech is secured (*Education (No.2) Act 1986* [4], s.43 [4]) this makes it more onerous, and potentially more legally hazardous, for them to deal with notices of this kind.

57. Do practices other than notice and take down appear to be more effective? ("notice and stay down", "notice and notice", etc)

We consider that notice-and-stay-down requirements are essentially impossible to comply with, since they will require all postings by all users to be manually checked. Automated

checks will be unable to identify when minor, but insignificant, changes have been made to a file and even requiring prior moderation of all activity by the original poster will not prevent material being re-posted by someone else.
We consider that the problems identified by the Law Commission for free speech and the public interest (see response to Q56) as well as the legal uncertainty for hosting services can best be resolved by a notice and counter-notice process. Here the initial notice requires take-down of the material, with notification sent immediately to the person who posted it. The poster may then issue a counter-notice, in which case the material will be replaced and the complaint resolved, if necessary, by legal action between the complainant and the poster. Hosting providers that abide by this process are excluded from liability.

58. Are you aware of cases where national authorities or legal bodies have imposed general monitoring or filtering obligations?

The UK's *Digital Economy Act 2010* [7] appears to oblige "subscribers", which may include businesses and providers of wireless networks, to implement monitoring and filtering to prevent their networks being used to breach copyright. Thresholds for appearance on the serious infringers list, and for future technical measures, have been designed for domestic connections used by a few members of a family, not for organisations with hundreds or thousands of users. Since the proposed notification regime means that only a very small proportion of complaints will actually be passed on to these organisations (a recent Ofcom consultation [8] proposed that only one complaint per month will actually be forwarded), organisations classed as subscribers cannot deal with individual infringers, so appear to have no option but to implement general monitoring and filtering of all their users. Discussions on when an organisation can claim the legal defence of having taken appropriate measures to prevent copyright breach have also concentrated almost exclusively on technical monitoring and filtering.
In the past Government Ministers have threatened to introduce legislation [9] requiring blocking of indecent images of children if this was not done voluntarily.
Elsewhere in Europe courts appear to have been willing to order ISPs, despite their mere conduit status under the Directive, to prevent access to sites or types of material, e.g. copyright (Belgium: *SABAM v Scarlett* [10]), gambling (France [11]). As in our answer to Question 69, these obligations may involve a requirement to monitor all traffic, depending on what is technically required to implement them: for copyright material it appears that monitoring and filtering is the only way to achieve the required block; for gambling it might be sufficient to prevent routing of traffic to certain websites, but reports suggest that ISPs will also be required to monitor traffic content in order to detect attempts to evade these blocks.

59. From a technical and technological point of view, are you aware of effective specific filtering methods? Do you think that it is possible to establish specific filtering?

We consider that filtering can only be effective if the user wishes to be protected from the material that is filtered.
Filtering will inevitably be ineffective when used for material that users wish to access, because internet technology will always provide simple ways for users to evade such filters. Encryption and indirect routing of traffic are both excellent ways to protect privacy of individual users and are now widely available in standard tools. These same technologies can also be used to make communications impossible to filter.
Filtering is also limited in its scope because the Internet permits many different models for the distribution of content. A filter that is designed to prevent the transfer of a single file from a server to a client is very unlikely to work if the same file is split into chunks that are distributed separately between clients.

60. Do you think that the introduction of technical standards for filtering would make a useful contribution to combating counterfeiting and piracy, or could it, on the contrary make matters worse?

As in our answer to question 59, we do not believe that filtering can be effective in preventing users accessing content that they want. Copyright material clearly falls into this category. Furthermore we believe that requiring such filtering would be damaging both to the safety of internet users and their computers and to the stability of network services. Implementing filtering to prevent access to copyright content, or any other type of content or service that users wish to access, will encourage more users to adopt filter-evading technologies as a routine part of their internet use. This will render all filters ineffective – not only those introduced to combat counterfeiting and piracy, but also those used by ISPs and other organisations to reduce the risk of exposure to content harmful to the users and their computers. Adult content and viruses alike would spread more easily around the Internet if this were to happen.

Implementing filtering on large and fast networks is technically challenging and can result in unexpected interactions. For example filtering systems used by ISPs to block URLs on the Internet Watch Foundation's (IWF) list of illegal images may send traffic to a website along a different network route if it contains an image on the list. Normally this change is invisible, but on a site that receives a large volume of legitimate traffic, the change in routing can create traffic hotspots and trigger attack prevention systems, as appears to have happened when the IWF listed a single page on Wikipedia in 2008.

61. Are you aware of cooperation systems between interested parties for the resolution of disputes on liability?

A pilot trial of a notice and counter-notice scheme was agreed between various rightsholder groups and members of the London Internet Exchange in 2004/5. However this did not proceed because the participant rightsholders were unable to identify any infringing content that was hosted on systems controlled by the participant ISPs. Since the pilot would have required the rightsholders to contract in advance that they would not enforce their legal rights against the hosting ISPs, this meant that it was not possible to proceed with the pilot.

62. What is your experience with the liability regimes for hyperlinks in the Member States?

63. What is your experience of the liability regimes for search engines in the Member States?

Current UK law is silent on potential liability for hyperlinks or search engines. Although we no direct experience of these liability regimes, enquiries received from our customers suggest that the resulting legal uncertainty is of concern to them. As in our response [12] to a UK Government consultation in 2005, we consider that the certainty provided by the Directive for hosting providers has been beneficial both for them and for claimants by encouraging the development of effective procedures for removal of problematic content and therefore that extending liability protection to hyperlinks and search engines would be likely to provide the same benefits.

64. Are you aware of specific problems with the application of the liability regime for Web 2.0 and "cloud computing"?

The problems of “actual knowledge” discussed in our answer to Q53 are particularly significant for sites hosting user-generated content (often referred to as Web 2.0). Such sites may wish to proactively edit or check the content that they host, however the current law encourages them instead to wait until problems are reported by a third party. This is often summarised as “better not to check at all than to check and miss something”. We consider that current law should be clarified or modified to ensure that a host of third party content does not lose liability protection by proactively checking for problem content.

Cloud computing adds further legal complexity, since different aspects of what appears as a single service will normally be controlled by different people who may be subject to different legal regimes. For example it would already be possible for a UK business to run its website on a cloud service hosted by a provider in France and to incorporate a user generated content component run by an organisation in the USA but hosted on a service in India. In such a system it is very unclear where liability does (or indeed should) fall, or which legal regime would apply.

65. Are you aware of specific fields in which obstacles to electronic commerce are particularly manifest? Do you think that apart from Articles 12 to 15, which clarify the position of intermediaries, the many different legal regimes governing liability make the application of complex business models uncertain?

Far from a “limited takeoff of electronic commerce”, the education and research sectors have experienced considerable growth in using and providing services on-line. Accessing commercial content – including audio-visual, photographic and written material – from the UK and abroad over the Internet is now a routine part of teaching, learning and research. Many content providers have been willing to enter into national agreements, for example using the JISC NESLi2 model licence [13]. Some problems have been encountered with different interpretations of Data Protection law, especially for resources hosted outside the EEA, and with copyright and licensing regimes that are subject to geographical boundaries, for example that permit access by students in university accommodation but not those living at home.

66. The Court of Justice of the European Union recently delivered an important judgement on the responsibility of intermediary service providers in the Google vs. LVMH case. Do you think that the concept of a "merely technical, automatic and passive nature" of information transmission by search engines or on-line platforms is sufficiently clear to be interpreted in a homogeneous way?

As in our response to Q53, there appears to us to be a risk that the requirement that the intermediary’s involvement be “merely technical, automatic and passive” may further discourage proactive searching or filtering for problem content. If providers conclude that it is legally safer to wait for a complaint then this would risk increasing the amount of problem content on networks and servers.

67. Do you think that the prohibition to impose a general obligation to monitor is challenged by the obligations placed by administrative or legal authorities to service providers, with the aim of preventing law infringements? If yes, why?

Legal and administrative authorities are placing increasing obligations on both hosting providers and ISPs. Whether these constitute a general obligation to monitor, contrary to the prohibition in EU law, depends on what is necessary in practice to fulfil them. We would consider that a duty that could be fulfilled by a one-off technical change (for example to disable routing of a particular Internet Protocol address) would not involve an obligation to monitor, whereas a duty that required repeated or continuous inspection of network traffic or content by a computer or human (for example to prevent the transmission of copyright material) would constitute an obligation to monitor.

Determining which category applies to a particular duty is complex because duties are rarely expressed in terms of technical requirements and those that are expressed in legal terms are

likely to change in nature as new technologies develop. For example a duty to “prevent access to content X” may be possible to satisfy with a technical change if X is only available on a single server, but will require continuous monitoring if X is being distributed though a peer-to-peer network.

We would note that there is a further problem with duties relating to copyright, since the concept of copyright cannot be expressed in purely technical terms. Precisely the same sequence of bits may breach copyright, or be lawfully licensed, or fall within one of the law’s exemptions (e.g. private study), depending on agreements and legislation existing outside the Internet sphere. Other than in very limited circumstances, therefore, determining whether or not a particular sequence of bits breaches copyright law is likely to require detailed examination both of the applicable laws (which may involve more than one jurisdiction) and of the agreements relating to the particular content.

68. Do you think that the classification of technical activities in the information society, such as "hosting", "mere conduit" or "caching" is comprehensible, clear and consistent between Member States? Are you aware of cases where authorities or stakeholders would categorise differently the same technical activity of an information society service?

We are not aware of any problems with different interpretation of these terms.

69. Do you think that a lack of investment in law enforcement with regard to the Internet is one reason for the counterfeiting and piracy problem? Please detail your answer.

Under UK law infringement of copyright may be either a criminal or civil matter. As far as we are aware, law enforcement bodies in the UK actively and successfully pursue those responsible for counterfeiting and piracy at the criminal level, so investment in these cases does not appear to be a problem. At the civil level, those who possess intellectual property rights are responsible for taking legal action to enforce them. Willingness to do this appears to vary considerably between different rightsholders. The original intention of what became the *Digital Economy Act 2010* [7] was to make it easier for rightsholders to target enforcement action on serial offenders. These provisions are still in the Act though, as they have been relatively little discussed, it is not known whether they will lead to an increase in higher-value civil actions by rightsholders when they come into force.

Links

[1] http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm
[2] http://www.out-law.com/page-11366
[3] http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf
[4] http://www.legislation.gov.uk/ukpga/1986/61/section/43
[5] http://www.legislation.gov.uk/ukpga/2006/11/contents
[6] http://www.lawcom.gov.uk/docs/defamation2.pdf
[7] http://www.legislation.gov.uk/ukpga/2010/24/contents
[8] http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf
[9] http://www.out-law.com/page-6937
[10] http://www.sabam.be/website/data/Press_Releases/SABAM_vs_TISCALI_engl.pdf
[11] http://www.out-law.com/page-11306
[12] http://www.ja.net/development/legal-and-regulatory/regulated-activities/related-regulatory-documents/janetuk-response-to-dti-consultation.html
[13] http://www.jisc-collections.ac.uk/nesli2/