



representing the  
recording industry  
worldwide

## ISPs - Technical Options for addressing online copyright infringement

IFPI estimated in 2006 that there are 20 billion illegal downloads of music files each year, far outstripping the developing legitimate digital market and presenting enforcement challenges for right holders. Developing cooperation with ISPs to address illegal downloads is key to the future of the music business.

This cooperation has not been sufficiently forthcoming from ISPs in Europe so far. In general, ISPs do cooperate with right holders in the specific circumstances where infringing content is hosted on their own servers, by removing or disabling access to the content in response to a notice (conduct incentivised by the safe harbour for hosting activity in the E-Commerce Directive). By contrast, infringing content hosted on user's computers and distributed via P2P networks presents greater challenges. Most ISPs do not take any steps to address the massive piracy of music on P2P networks. In addition, most do not do enough where infringing content is hosted on websites located overseas, sometimes in rogue jurisdictions where no effective enforcement mechanisms are available.

Whatever the structure of the specific piracy problem, every person that accesses the internet must do so through an ISP, and each ISP has complete technical and commercial control over the traffic that is generated by its own customers.

There are a number of feasible and reasonable options available to ISPs to help address copyright infringement on their networks that can be supported by technology solutions. ISPs already implement technology to manage traffic across their networks for their own self-interest: for example most ISPs filter email traffic to remove spam, and many ISPs "throttle" (slow down) traffic on P2P networks at busy times to reduce bandwidth costs.

At a basic level, there are at least three technical options available to ISPs to control infringing traffic, which can be implemented in various ways to enforce the ISP's copyright policy. None is overly burdensome or expensive, or causes problems for regular services to the ISP's customers. These options are not mutually exclusive, and could be implemented across an ISP's entire network, or at the level of an individual user or users, in conjunction with a graduated response program. A complete solution to piracy would involve elements of all three options.

1. **Content filtering:** This would involve the ISP placing an automated appliance at an appropriate point in its network to process traffic, identify audio files, and match them against a reference database of "audio fingerprints" for legitimate sound recordings. Unlicensed files that are a "match" for copyright sound recordings in the database would be blocked and could not be exchanged over the ISP's network. The components needed to implement content filtering - the audio fingerprint technology and the databases of reference fingerprints - are already well developed and are in use on P2P networks including Kazaa and iMesh. A judge in a Belgian court, deciding the case of SABAM v Tiscali, recently considered an expert report including a number of technical options and found that that content filtering is an effective and not unreasonably burdensome measure for an ISP to implement to address P2P piracy.
2. **Protocol blocking:** Again this would be implemented with the help of an automated appliance which would detect the "protocol" associated with various types of traffic, and block objectionable traffic. For example, web and email traffic has a different protocol to P2P traffic, and different P2P services can be distinguished from one another by their protocol. It is therefore possible for ISPs to block their customers' access to specific P2P services that are known to be predominantly infringing and that have refused to implement steps to prevent infringement, while not affecting regular services such as web and email.

3. **Blocking access to infringing online locations:** This solution involves an ISP blocking access for its own customers to specific infringing websites, services or online locations that are hosted overseas or at another ISP. The solution could apply to websites, especially those in rogue jurisdictions or that refuse to cooperate with right holders (for example, The Pirate Bay, an infamous infringing service located in Sweden). There is no doubt that this solution is technically feasible. Some ISPs already block access to websites that contain pornography (e.g. the service provider Scarlet in Belgium), and in 2006 a Danish court ordered an ISP to block access to the Russian website [www.allofmp3.com](http://www.allofmp3.com).

While there is no doubt that these technical steps are feasible and would, if implemented, dramatically reduce the level of music piracy, it is important to realise that no technology is in itself a 100% complete fix to the piracy problem. It is essential that technology is the tool to implement an ISP's policy of addressing piracy on its network rather than a solution in itself.

This paper provides only a general overview of these technical options; more detail is available from IFPI on request.