# Intermediary Service Providers – the next "big brothers"?

*by Dr. Paul Micallef Grimaud, B.A., M.A., LL.D.**

Intermediary Service Providers (ISPs) in EU Member States have traditionally enjoyed a comfortable position of no responsibility with respect to the content transmitted through the use of the services provided by them. However, various recent judgments delivered by national courts in a number of Member States, have disturbed this harmonised position and have shone the spotlight on ISPs and their responsibility in combatting online crime.

The position of ISPs and their legal responsibilities in relation to the data transmitted and accessed by users of their services, is regulated by the Electronic Commerce Directive[1], which seeks to achieve a homogeneous application of the underlying principles throughout the various Member States.

The Directive creates a three-tiered structure aimed at regulating the different levels of control that the ISPs may have over the information transmitted and accessed through their services.

**Mere Conduit**

The principle of "Mere Conduit" applies to those ISPs whose role is limited to the transmission of information provided by a recipient of the service, or the provision of access to a communication network.

Such services are construed to include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and that the information is not stored for any period longer than is necessary for the transmission.

In accordance with Article 12 of the Directive, such ISPs are not to be held responsible for the content conveyed through their services provided that said service providers do not initiate the transmission, select the recipient, or select or modify the information contained in the transmission.

The Directive does not however restrict a Member State's courts and authorities from requiring the service provider to take those steps that are necessary to block the transmission of the unlawful content.

**Caching**

The notion of "caching" refers to the automatic, intermediate and temporary storage by the ISP of that information held in transit, for the sole purpose of making the information's onward transmission to other recipients more efficient.

[1] Directive 2000/31/EC

Article 13 of the Directive protects the service provider from incurring liability where its involvement with the unlawful information is limited in the above manner. Such an exclusion of liability stands on condition that the provider does not modify the information, complies with the conditions relative to the access of information, complies with rules regarding the updating of information, does not interfere with the lawful use of technology and acts expeditiously to remove or disable the access to the information that it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Once again the Directive does not restrict Member State's courts and authorities from requiring the service provider to take those steps that are necessary to block or remove access to unlawful content.

**Hosting**

The Directive refers to "hosting" as a service consisting of the storage of information provided by a recipient of the service.

Article 14 of the Directive states that the ISP providing hosting services shall not be held liable for the information stored at the request of the recipient of the service as long as the ISP does not have actual knowledge of the illegal activity or information and is not aware of the facts or circumstances from which said illegal activity or information is apparent. Moreover the ISP is exempt from liability where upon obtaining such knowledge he acts expeditiously to remove or disable access to such information.

Once again the Directive does not restrict the Member States' courts and authorities from requiring the service provider to terminate or prevent an infringement, nor does it preclude the Member States from establishing procedures governing the removal or disabling of access to information, otherwise known as 'Notice and Take Down' Procedures.

**The overarching Exemption**

In addition to the above individual exemptions offered to the three forms of ISP activity, Article 15 of the Directive provides an overarching exemption from liability that applies to all three forms of activity.

Article 15 provides that Member States shall not impose a general obligation on ISPs (as understood by articles 12, 13 and 14) to adopt a "big brother" stance and monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity. This principle reflects a reasonable cognisance of EU policy makers of the impracticality of burdening ISPs with the task of privately policing and censoring the internet.

**Current Trends**

In June 2007, upon a request by the Belgian Society of Authors, Composers and Publishers (SABAM), the Court of First Instance in Brussels ordered Scarlet Extended Ltd (previously Tiscali) to put an end to the copyright infringements through the illegal sharing of its customers,

by way of P2P software, of electronic files containing a musical work belonging to SABAM's repertoire, by implementing filtering software and blocking mechanisms. Scarlet was also ordered to notify SABAM in writing of the measures it would be applying with a view to respecting this decision. Scarlet was given 6 months to conform to this decision, on pain of incurring a daily fine.

In laying down this order the Court insisted that the termination order did not impose on Scarlet a general obligation to monitor its network but that the solutions identified are "technical instruments" that limit themselves to blocking or filtering certain information transmitted on the network.

Scarlet appealed the said order before the Court of Appeals of Brussels. During this case, the Belgian Internet Service Providers Association (ISPA), and the major internet service provider Belgacom, intervened in the proceedings. Scarlet argued the disproportionality of the order to filter all P2P traffic, and the complete ineffectiveness of the requested measure. Scarlet also argued that the systematic surveillance of internet users by their ISPs was illegitimate.

On the 25 January 2010, the Brussels Court of Appeal referred the case to the European Court of Justice for a preliminary ruling on two questions. The ECJ was requested to clarify whether, in view of the E-Commerce Directive, national courts may order ISPs to filter the peer-to-peer traffic of their customers and, if copyright infringements are detected, to block the transfer of the infringing files. Secondly, the ECJ was requested to clarify whether a national court should, when imposing this measure, apply the proportionality principle when judging the effectiveness and deterrent nature of the measure. To date the ECJ's judgment has not been delivered.

June 2007 saw yet another judgment challenging the traditional "comfort-zone" enjoyed by ISPs in relation to the information transmitted through their services. This time it was the Paris Court of First Instance that condemned MySpace for having stored and having provided public access to certain videos without the right holder's authorisation. In its judgment, the Court circumvented the protection afforded to hosts under the E-Commerce Directive by concluding that although MySpace performed the technical function of hosting, it could not be considered as a host provider under the E-Commerce Directive since, the fact that it was financed through online advertisements on its website and that MySpace's website was equipped with a specific lay-out and presentation, made MySpace more akin to an "*éditeur de contenus*" or "content publisher". Consequently MySpace was ordered to pay the rights' holder dmages for infringement of his Intellectual Property rights.

In another judgment, known as the *Dailymotion* case, the Paris Court of First Instance concluded that a video-sharing website provided the tools to infringe copyright rules and hence could not benefit from the indemnity afforded to hosts. In this case Dailymotion was sued for having stored a cinematographic work on its platform that was put online without authorisation by the right holder. The Court held that defendant should have realised the illegal activity going on through the provision of its services and was duty bound to prevent this from happening. Hence the Court concluded that it could impose a general monitoring obligation on Dailymotion notwithstanding the provisions of the E-Commerce Directive.

The Paris Court of Fisrt Instance delivered yet another judgment in this series of damning judgments. In the *Google* case, the search engine Google was condemned for not having

undertaken sufficient efforts to remove footage from its Google Video service when, after having actually removed the litigious footage, the same footage was later posted again. According to the court, although Google had qualified as a provider of hosting services, it could not invoke a liability exemption since, once a provider has been informed of the illegal nature of a certain footage posting, it must take all measures necessary to ensure that any future "re-postings" of such footage will be prevented.

The Antwerp Court of First Instance, too, has left its mark in this string of judgments whereby, in the *Seniorennet* case it held that any operator of a platform has the obligation to take reasonable action to prevent damage from occurring to third parties. Hence, although defendant in this case was not found liable for breach of copyright he was ordered by the Court to put in place all those procedures necessary to prevent future exchanges of illicit content from occurring.

In the *Rapidshare case,* the German Dusseldorf District Court followed the reasoning adopted by the Belgian Court in the SABAM case, ordering RapidShare to take mandatory action to prevent further infringement of copyrighted works.

The ISP industry groups have criticised these pressures to adopt monitoring techniques. Their position is well summarised in a statement issued by the Internet Service Providers Association of Ireland, in reaction to a lawsuit filed in March 2008 by EMI, Sony and Universal against Ireland's largest ISP, Eircom. The suit demands that Eircom be compelled to install filtering technology to prevent further infringement of plaintiffs' copyrights.

"The Association is totally opposed to any obligation (such as that apparently in this Belgian court decision) that ISPs should monitor their customers' Internet communications on the off-chance that someone may be distributing copyrighted work which they do not have permission to use. (How is an ISP, or any other third party, to know whether a communication is copyrighted, who owns the copyright or whether permission has or has not been granted?) The privacy of all personal and business communications is at stake here. This is the electronic equivalent of the post-office steaming open every letter in the sorting office, checking the contents and never delivering the bits some unknown worker believes should be censored. If legislation forced ISPs to monitor, never mind the democratic or moral issues, in practice everyone would immediately switch to encryption rendering any such monitoring useless, the monitoring process itself would slow the Internet to an unusable snail's pace."[2]

**Where does this leave us?**

With various courts in individual Member States adopting positions that diverge considerably from that laid down in the Electronic Commerce Directive, it is very hard, if at all possible, to speak of a harmonised legal position in relation to ISP liability.

Maltese law[3] faithfully reproduces the above-mentioned provisions of the Electronic Commerce Directive. However, in the light of the judgments described above that have steered away from the wording of the Directive, Maltese ISPs have little comfort that our Courts will not adopt a position similar to that adopted by courts in other Member States and be requested to play a

[2] IRISH TIMES, Eircom taken to court over illegal music downloads March 10, 2008
[3] The Electronic Commerce Act, Chapter 426 of the Laws of Malta

more proactive role in the combatting of the illegalities committed by end users through the use of the services provided to them by ISPs.

---

* *The Author is a member of the Litigation Practice at Ganado & Associates, Advocates. His areas of specialistaion include IT & Telecoms Law.*