Remfry & Sagar

ATTORNEYS-AT-LAW

TRADE MARKS • PATENTS • DESIGNS • COPYRIGHT

Remfry House at the Millennium Plaza
Sector 27, Gurgaon - 122 009
New Delhi National Capital Region, India
Tel : 91-124-280 6100 Fax : 91-124-280 6101 & 257 2123
E-Mail: remfry-sagar@remfry.com
http://www.remfry.com

376-B (Old No.202)
Avvai Shanmugam Salai, Gopalapuram
Chennai - 600 086, India
Tel & Fax : 91-44-4263 7392
E-Mail : remfry-sagar@remfry.com
http://www.remfry.com

Endless flotillas and safe harbours: perspectives on ISP and host liability

Author
Vishnumohan Rethinam

The Internet pervades every aspect of our lives. From communication to commerce, it promises limitless access to continually evolving worlds of information, products and services. It is akin to our expanding universe without any foreseeable limits.

In this complex, coded and pixelated space, merchants ply their trade and offer a wide variety of goods and services to customers. As is the case with traditional brick-and-mortar models, deals can sour and disputes can arise. In brick-and-mortar models, liability is generally attributed to the producer or service provider whose act or omission has resulted in injury to the plaintiff – although it is not unheard of for intermediaries (eg, distributors or wholesalers) to be roped in.

In cyberspace, intermediaries are commonly accused of contributory infringement. Cases involving internet service providers (ISPs) and hosts, including search engines and social media companies, are well documented. Jurisprudence on this issue varies globally.

This chapter examines instances of liability attributed to intermediaries and prevailing global trends in dispute resolution.

ISPs and hosts

An ISP provides a subscriber with internet access. It may provide other services, such as tools and space to host websites and email accounts. In IT vernacular, a 'host' can have multiple meanings; however, the most suitable definition for the purpose of this chapter is a computer or network where third-party websites and applications are hosted. An ISP can provide hosting services and vice versa.

There are two generally accepted reasons why these service providers are sued in addition to or instead of the parties directly responsible for infringement:

- An actual infringer can be hard to locate, whereas a service provider is usually an incorporated entity with an accessible address; and
- The theory that a service provider cannot disclaim responsibility for the content it carries places liability for that content on the service provider.

Of course, in reality, the perceived deep pockets of service providers motivate attachment of liability at least as much as the reasons listed above.

Service providers have traditionally argued that, even with the most advanced technological resources available, it is virtually impossible to filter potentially infringing content at the threshold. Even if it were possible, it would be extremely difficult to determine, without prior notice, whether such content was being used without authorisation. Even assuming that service providers could assimilate resources to verify content at the threshold, it is generally accepted that this would deter clients and be commercially unviable in the long term.

The following illustrative examples have contributed to global jurisprudence in this area.

United States

In the 1995 decision *Religious Technology Center v Netcom On-line Communication Services Inc*, the plaintiff sought to injunct the actual alleged infringer, the host (a paid bulletin board service (BBS)) and the ISP (Netcom) for copyright infringement. On being served notice by the plaintiff, the host challenged the plaintiff's right to the allegedly infringed works and the plaintiff failed to respond. The ISP refused the plaintiff's request to disallow the alleged infringer access to the Internet on the basis that this would potentially deter other subscribers to the host's BBS. The ISP also contended that it would be impossible to pre-screen the allegedly infringing posts; further, the plaintiff presented no evidence that the ISP could have pre-screened the postings.

The court dismissed the plaintiff's request for a preliminary injunction based on the direct infringement claim. However, it did not decide on the plaintiff's claim of contributory infringement and left the issue open to trial. The case eventually settled.

This case, among others, led to the passing of the Digital Millennium Copyright Act, which provides 'safe harbour' provisions (ie, exemption from liability) to online service providers such as ISPs and hosts, subject to the following conditions:

- The service provider must not have actual knowledge of the infringing activity;
- Where the service provider has the right and ability to control the infringing activity, it must not receive a financial benefit directly attributable to the infringing activity; and
- On receiving proper notification of claimed infringement, the service provider must expeditiously take down or block access to the material.

In *IO Group Inc v Veoh Networks Inc* an internet network allowed its subscribers to share video content on its site. The plaintiff alleged copyright infringement, including contributory infringement, in the defendant's acts of streaming videos over which the plaintiff owned copyright. The judge allowed the defendant's motion for summary judgment on the grounds that it could avail of the safe harbour provisions of the Digital Millennium Copyright Act.

> **Even assuming that service providers could assimilate resources to verify content at the threshold, it is generally accepted that this would deter clients and be commercially unviable in the long term**

The judge stated: "The court does not find that the Digital Millennium Copyright Act was intended to have Veoh shoulder the entire burden of policing third-party copyrights on its website (at the cost of losing its business if it cannot). Rather, the issue is whether Veoh takes appropriate steps to deal with copyright infringement that takes place. The record presented demonstrates that, far from encouraging copyright infringement, Veoh has a strong [Digital Millennium Copyright Act] policy, takes active steps to limit incidents of infringement on its website and works diligently to keep unauthorized works off its website. In sum, Veoh has met its burden in establishing its entitlement to safe harbor for the alleged infringements here."

In *Viacom International Inc v YouTube Inc* – a major case which is generally accepted to have tested the limits of the Digital Millennium Copyright Act's safe harbour provisions – Viacom sued YouTube and its parent Google for copyright infringement, alleging that they had facilitated the uploading and viewing of tens of thousands of unauthorised proprietary video clips. The defendant claimed safe harbour under the

Digital Millennium Copyright Act, including compliance with thousands of takedown notices sent to it by the plaintiff. The district court agreed with the defendant and issued summary judgment in its favour. On appeal, the matter was remanded to the district court, with the indication that there was enough material to warrant a trial. However, the appeal court stated that YouTube was protected from liability, except where it actually knew of (or was wilfully blind to) specific instances of infringement (although one might question how this could be firmly established absent takedown notices). On remand, the district court re-examined the issues raised by the appeal court and again issued summary judgment in the defendant's favour. Its second-instance ruling seems to indicate that without takedown notices, defendants are not required to take action to claim safe harbour under the Digital Millennium Copyright Act. The case eventually settled.

European Union

In the European Union, analogous provisions of the EU E-commerce Directive (2000/31/EC) address the liability of intermediaries. Article 14 of the directive (which refers to hosting) requires member states to ensure that a service provider is not liable for information stored at the request of a customer, on condition that the provider:

- has no actual knowledge of illegal activity and, in the case of claims for damages, is unaware of the facts or circumstances which make the illegal activity apparent; and
- on becoming aware of the illegal activity, acts expeditiously to remove or block the infringing information.

In *L'Oreal v eBay* the European Court of Justice (ECJ) had occasion to opine on the applicability of Article 14. It ruled that Article 14 applies to hosting providers if they do not play an active role which would allow them to have knowledge of or control over the stored data. The ECJ stated that being in the business of providing a service and being paid for that service does not disentitle the provider from claiming exemptions from liability provided by the directive. It further stated that the situation would be different if the service provider assisted customers in optimising the presentation of certain information or promoted certain information.

In *Twentieth Century Fox v British Telecommunications (BT) PLC*, the UK High Court ordered BT (the service provider) to prevent access to Newzbin.com, a website that allowed access to copyrighted content without authorisation.

The plaintiff had previously been granted an injunction against Newzbin, which operated Newzbin1 at www.newzbin.com. Following the injunction, although Newzbin1 ceased operations, Newzbin2 surfaced. On this occasion, plaintiffs sought an order against BT directing it to block users from accessing Newzbin1 and Newzbin2.

Given the previous decision against Newzbin1, the court held that BT had knowledge that subscribers were using its service to commit copyright infringement.

The court explained that the requirement for actual knowledge should not be interpreted too restrictively. Each specific instance of infringement need not be known to the provider; it will suffice that "the service provider has actual knowledge of one or more persons using its service to infringe copyright".

Article 15 of the E-commerce Directive states that member states may not oblige service providers to monitor information or actively investigate facts or circumstances indicating illegal activity. In *Sabam v Netlog* the ECJ ruled on a reference from a Belgian court petitioned by Sabam requesting an injunction requiring Netlog to install a filtering system to detect and prevent copyright infringement. The ECJ held that such an injunction would contravene Article 15.

The ECJ held that: "such an injunction would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly."

India

Exemption from liability for service providers is provided under Section 79 of the IT Act 2000. Section 52 of the Copyright Act 1957 also contains analogous provisions.

Section 79 of the IT Act provides that a service provider is not liable for any third-party information, data or communication link made available or hosted by it in the following circumstances:

- The service provider provides access to a communications system over which information made available by third parties is transmitted or temporarily stored or hosted; or
- The service provider:
  - does not initiate the transmission, select the receiver of the transmission or select or modify the information contained in the transmission; and
  - observes due diligence while discharging its duties under the IT Act, as well as observing any other guidelines prescribed by the government.

Section 79 further states that the exemption cannot be claimed if the service provider:

- conspires in, abets or induces the commission of unlawful acts; or
- on receiving proof (eg, in the form of a takedown notice) or being notified by the government that any part of its network is being used to commit an unlawful act, fails to remove or block that material in a timely fashion and without vitiating its evidentiary value (Section 79(3)).

The IT (Intermediaries Guidelines) Rules 2011 supplement Section 79 of the IT Act. Rule 3 defines what service providers' terms of service must include. Rule 3(2) indicates that the terms of service must warn users not to host, display, upload, modify, publish, transmit, update or share any information that infringes patents, trademarks, copyright or other proprietary rights. Rule 3(4) provides for infringing material to be taken down within 36 hours and for the preservation of records (for investigation purposes) for 90 days from the date on which the service provider learns of the infringement.

These provisions have generated much debate in the Indian legal community.

In *Shreya Singhal v Union of India* the constitutional validity of Section 79(3)(b) and Rules 3(2) and 3(4) was challenged before the Supreme Court. The petitioner stated that a service provider is called on to exercise its own judgement under Rule 3(4) before disabling information, in contravention of Rule 3(2). The petitioner claimed that this requirement:

Vishnumohan Rethinam
Partner
vishnu.rethinam@remfry.com

Vishnumohan Rethinam is a partner in the firm's trademarks department, where he is engaged in contentious and non-contentious work, including prosecution, oppositions, cancellations and appeals before the Trademarks Office and the Intellectual Property Appellate Board. He also heads the copyright department. His qualifications include a bachelor's in French (honours), a bachelor of laws and a master's in business law.

Counselling clients across a wide spectrum of industries, he facilitates complex negotiations and develops and implements enforcement strategies. He writes and speaks frequently on varied IP subjects, with an emphasis on trademarks and copyright on the Internet. He serves on the International Trademark Association Amicus Committee and the Federation of Indian Chambers of Commerce and Industry IP Committee.

- was vague and "over broad";
- presented the service provider with no opportunity to be heard; and
- had no connection with the subjects specified under Article 19(2) of the Constitution, which concerns the fundamental right to free speech and expression.

The Supreme Court compared analogous provisions under Section 69A of the IT Act, dealing with the government's power to issue directions to block public access to any information through any computer resource. It stated that under Section 69A, blocking can take place only via a reasoned order after complying with procedural safeguards, after hearing the originator of the information and the service provider.

Thus, Section 79 was 'read' with analogous safeguards to mean that the intermediary, on receiving actual knowledge that a court order has been passed asking it expeditiously to remove or disable access to certain material, must then fail to do so in order to be denied the exemption under Section 79. The Supreme Court stated that: "otherwise it would be very difficult for intermediaries to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not...the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79... The knowledge spoken of in the said sub-rule must only be through the medium of a court order."

In *Super Cassettes v MySpace* the Delhi High Court granted an injunction against the defendant, MySpace, on grounds of copyright infringement. The defendant facilitated content sharing by its users. The plaintiff alleged that the defendant had facilitated sharing of its copyrighted content. The defendant argued that it had no actual knowledge of the infringement; nor could it track infringing material while it was being uploaded. It also argued that the plaintiff had refused to register with its rights management tool, which would have facilitated the takedown of infringing material. Interestingly, the defendant's arguments of safe harbour under Section 79 of the IT Act were rejected on the basis that Section 81 of the IT Act states that nothing contained in the act can restrict anyone from exercising any right under the Copyright Act. The case is under appeal.

Conclusion

It is obvious that globally, laws and courts are trying to balance the interests of rights holders and service providers by recognising inherent difficulties for intermediaries attempting to detect IP infringement absent information from the rights holder. Without prejudice to any technological advances that may have taken place, there can surely be no foolproof method for a service provider to check independently whether a rights holder has granted permission to a user to upload a protected work. In the inevitably free-wheeling world of information and technology, vigilance and diligence would seem to be keywords for both rights holders seeking to protect themselves from sustained infringement and service providers seeking to dock in safe harbours. **WTR**

Remfry & Sagar
Remfry House at the Millennium Plaza
Sector 27, Gurgaon-122 009, New Delhi NCR
India
Tel +91 124 2806100
Fax +91 124 2806101
Web www.remfry.com