E

WIPO/INT/SIN/98/10
ORIGINAL: English
DATE: April 1998

THE REPUBLIC OF SINGAPORE

WORLD INTELLECTUAL PROPERTY ORGANIZATION

WIPO SEMINAR FOR ASIA AND THE PACIFIC REGION ON THE INTERNET AND THE PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

organized by
the World Intellectual Property Organization (WIPO)

in cooperation with
the Ministry of Law,
the Attorney-General's Chambers,
the National Science and Technology Board,
the Singapore Productivity and Standards Board

and
the Singapore Trade Development Board
of the Government of the Republic of Singapore

Singapore, April 28 to 30, 1998

V. INFRINGEMENT AND ENFORCEMENT OF IPRS ON THE INTERNET

Document prepared by Mr. Alban Kang, Alban Tay Mahtani and De Silva, Singapore
(with acknowledgement to Mr. A. Hooi for his assistance)

I. WHICH JURISDICTION APPLIES TO INFRINGING ACTS?

Jurisdiction normally lies in the courts of the country where infringement takes place. Hence, whether there is infringement of copyright, trade mark or patent depends on whether the nature of the act itself is an infringing act as determined by the laws of the country where the act takes place. Upon consideration of the present situation in relation to copyright and other intellectual property rights, the question of what the applicable law and jurisdiction on the information superhighway needs to be dealt with.

Copyright is territorial in nature. That is, if an infringement occurs in Singapore, Singapore laws apply. If someone in France downloads pictures copyrighted in the U.S., the key question to ask is where the reproduction takes place. In most cases, local laws would apply, that is, where the release of information occurs. Hence, the person in the above situation would be subject to French laws. The American plaintiff would then be faced with going to France to bring his action, especially if the defendant has no connections with the U.S.. The problem is compounded if the infringement occurs across a number of jurisdictions.

Furthermore, to bring a suit for copyright infringement, one must ask whether copyright subsists in the work. If the work is unpublished, the question of subsistence of copyright turns on where the author is resident or nationalized. If the work is published, it may be necessary to consider where it was first published. Singapore now recognizes first publication in 129 countries.

Whether copyright should, or can, remain territorial is the crux of the question. It has been suggested that conflicts of laws could be resolved through a more functional approach to the issues. Choice of laws analysis has traditionally led courts to look to the territorial situs of the acts that copyright law theoretically entitles authors and their successors to control. It was argued that in the shift from geographical space to cyberspace, judges may better apply the laws in effect on territories where remedies, in practice, can most adequately redress the violation of rights[1]. In any case, further harmonization of intellectual property laws would go a long way in the protection of our rights.

II. WHAT ARE THE LIABILITIES OF ISPS OR WEB PUBLISHERS WHO INDIRECTLY FACILITATE COPYRIGHT INFRINGEMENT?

The liability of Internet Service Providers ("ISPs") in regard to the content of their domain addresses and the liability of Web publishers in regard to the content of their websites is a practical area with direct consequences on the dissemination of information over the Internet. Hence, it is necessary to define the scope of liability of the ISP with regard to material that, for example, infringes copyright. Developments in this area has been spearheaded by U.S. cases. In *Sega Enterprises v Maphia*[2], the Defendant was held to have infringed copyright by operating a computer bulletin board from which users were uploading and downloading copies of Sega's copyrighted video games without the authorization of Sega.

---

1 Paul Edward Geller, *Conflicts of Law in Cyberspace: International Copyright in a Digitally Networked World (The Future of Copyright in a Digital Environment)*, 1996, Kluwer Law International (pub)

2 857 F Supp 679 (ND Cal 1994)

The evidence showed that the defendant was perfectly aware of the use of his bulletin board for that purpose. In *Playboy Enterprises Inc. v Frena*[3], the defendant's bulletin board distributed unauthorized copies of photographs from the *Playboy* magazine. The defendant was held to have infringed *Playboy*'s copyright, even though he claimed that he did not himself put such material on his board and was unaware that some of his subscribers were doing so. The mere fact that he was making copies available was an infringement. Also, the fact that subscribers were able to view the photographs on their computer screen constituted an infringement of the public display right.

The liability of a Usenet (a network of newsgroups on a bulletin board) operator was dealt with in the important decision of *Religious Technology Center* ("RTC") *v Netcom Online Communications Services* ("Netcom")[4]. The issue was whether Netcom, which allowed a bulletin board service ("BBS") critical of the Church of Scientology to reach the Internet, should be liable for copyright infringement committed by a bulletin board subscriber. RTC owned the copyrights in the unpublished works of L Ron Hubbard. A former minister of the Church, Erlich, posted the copyrighted works using a Usenet newsgroup as a forum for discussion and criticism of the Church. Both the BBS and Netcom were named as defendants in the matter. The federal judge decided that Netcom may be liable to the Church of Scientology for copyright violations committed by a subscriber. Knowledge was essential in establishing liability based on contributory infringement.

There have been other cases where the courts have based liability in this area on the level of control the ISP or Web publisher has over the subscribers. Whilst the ISP can put up disclaimers, a duty to monitor the content of the websites to a reasonable extent has been imposed. The common law duty should be compared with the statutory duty to monitor the content of the site for other offensive material like pornography.

In Singapore, all ISPs and Internet Content Providers are subject to the Internet Code of Practice, issued by the Singapore Broadcasting Authority under the powers conferred by section 18 of the Singapore Broadcasting Authority Act (Cap 297). Briefly, an ISP discharges his obligations under the code if:

(i) in relation to programs on the World Wide Web, he denies access to sites notified to him by the Authority as containing prohibited material;

(ii) in relation to Internet Newsgroups, he refrains from subscribing to, or unsubscribes from any newsgroups as the Authority may direct;

(iii) in relation to private discussion fora hosted on his service (e.g. chat groups), he chooses themes not prohibited by the guidelines; or

(iv) in relation to programs on his service contributed to by other persons (e.g. bulletin boards), he denies access to any contributions that contain prohibited material that he discovers in the normal course of exercising his editorial duties, or is informed about.

---

3 839 F Supp 1552 (MD Fla 1993)

4 No. C-95-20091 RMW, N.D. CA November 21 1995

With regard to (iv), the burden of monitoring is that he "discovers in the normal course of exercising his editorial duties". This does not place an unreasonably heavy burden on the ISP. Prohibited material includes material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws.

The Schedule goes on to describe the nature of prohibited material envisaged, being primarily pornography of sorts. However, the definition of prohibited material is broad enough to cover politically sensitive material, which is the precise form of censorship that many are concerned about. Furthermore, and rather unfortunately, the Schedule says nothing about the nature of copyright infringing material. Hence, whilst copyrighted material may be prohibited material under the broad umbrella of material being against the public interest, there should perhaps be greater definition of the liability of ISPs. Protection of material and content on the Internet should be in the nature of protecting the rights of individuals, as opposed to the curtailment of those rights.

Under section 139 of the Copyright Act, it shall be an offence to publish or cause to be published in Singapore an advertisement offering to supply in Singapore infringing copies of computer software even if the publication was made from outside of Singapore. A transmission of the computer program that, when received and recorded, will result in the creation of a copy of the computer program shall be deemed to constitute the supply of a copy of the computer program at the place where the copy will be created. If a Web site contains such infringing programs and the Web site proprietor knew that the programs contained at the site were infringing software, an offence would have been committed. The question then remains whether the liability can be imputed to the ISP of the web-site. It would seem however, that bulletin board operators, being in closer contact or control of their BBS content, might be potentially liable.

Most recently, the EC (Electronic Commerce) Policy Committee, suggested that an ISP should not be liable for third-party content that is outside its control and for which it merely provides access.[5] As an example, one committee member said that the ISP should not be penalized for defamatory contents posted on an Internet discussion group. Whether it is entirely desirable to exclude the ISP from all responsibility is questionable.

III. IMPACT OF THE INTERNET ON ENFORCEMENT

Perhaps the most important question with regard to enforcement on the Internet is whether policy makers should adopt the path of building fences, as opposed to preserving the barrier free nature of the Internet. Knowing your rights can only make sense if you have the means and mechanism to be able to enforce those rights. In the absence of concrete legislation specially tailored to cope with this or policy statements by the various governmental departments, this area of law has already begun to evolve on its own. This is perhaps the best

---

[5] See *Private Sector urged to take lead in Electronic Commerce Drive, Business* Times Onlive, 14 April 1998.

indication of the necessity of formulating the right legal structure to deal with the rapidly emerging situation.

The identity of the infringer and the place where the infringement takes place are real issues in the area of enforcement. However, the present system cannot be seen to be the final solution. As the Internet presents a real challenge to existing concepts and definitions to intellectual property law, a new and wider approach should be taken to address the situation within the new environment of the Internet.

Traditionally, identifying the infringer has not been as daunting a task as in the context of the Internet. Take the example of copyrighted materials within an email. The infringer sending out the infringing materials through email may do so from behind an anonymous remailer. The anonymous remailer offers the service of stripping identifying material from emails and passing them on, all done automatically, without the need for any human instructions. "Spoofing" occurs when someone uses a false email identity, with or without a false IP address. The IP address would still enable the sending computer to be identified, or that the sender was a subscriber to a particular commercial ISP. However, spoofing is but a concern with procedure, which can be properly addressed by implementing stricter identification requirements when applying for a new account and placing prohibitions against sharing accounts (much like keeping ATM PIN numbers to yourself). The larger problem of whether there is adequate protection against infringement remains. There should a more defined means of linking each identified account with an act of infringement in a particular location or jurisdiction.

In this respect, the courts, as outlined above, have been willing to hold a third party host responsible for infringement. However, whilst the host may be liable for infringement, the period for which the host may be responsible would only be to the extent that they are able to reasonably monitor the contents of their sites. To this end, the extent of control is also relevant. However, for that brief period where the ISP, for example, is not aware of the infringing material posted, the harm and damage to the right-owner might already be substantial. Hence, it is necessary to look to the primary infringer, the individual directly responsible for the posting, in order to strengthen intellectual property rights on the Internet.

Infringing material often stays on the Internet for very short durations. This poses difficulties for right-holders who have to move fast to contain the damage. The onus of protecting their own rights shifts onto the right-holder himself. This could be analogous to the copyright owners of musical works. Collecting agencies, like the IFPI, have been set up to collect royalties, for example, on the behalf of the right-owners. This would substantially decrease the almost impossible burden of the individual right-owner. The question is whether a private solution should be adopted to cope with this problem of the Internet. Even then, statutory safeguards should be available to regulate such a set-up.

The other issue with the Internet lies in the transportability of sites. Sites on the Internet may just as quickly reappear out of jurisdiction, available to the same, and perhaps wider, audience than before. If a right-owner has an injunction against an infringer, can he do anything to deny people access to the infringing site if it reappears out of the jurisdiction. The pertinent question would then be how far should the extent of the injunction reach, especially if jurisdiction for the injunction lies in the location of the original site.

To require ISPs in a particular jurisdiction to block out particular sites from another location inevitably goes towards the building up of "fences". However, blocking out a whole site may be viewed by some to be too extreme a measure to adopt. Arguments similar to those objecting to blanket censorship have been made. Singapore's ISPs are already in the practice of using proxy servers to block out banned sites on the list of the Singapore Broadcasting Authority.

"Fences", used as an analogy by reference to barriers built across real property, include contractual arrangements by which one party gives the other access, under strict conditions, to a trade secret in his possession.[6] Legal sanctions act as partial fences as well. With regard to software, updating policies restricting use to registered users of legitimately acquired copies of the product, in conjunction with other measures, are partial fences as well. Fences used in this sense include various sanctions and measures to protect one's property right. In our context, it defines and protects our intellectual property rights.

Fences are only effective if they are able to protect our rights and prevent a corrosion of the property right. Our present fences, or boundaries, of our intellectual rights if not redefined might be ineffective in the face of the digital revolution, information technology and the Internet. The international community has recognized, through the long-standing Berne Convention, and TRIPS, and most national laws, that the protection rather than the pilfering of intellectual works is the way to encourage their creation, improvement and dissemination. This should not change because of the Internet. Protection should in fact be raised to cope with the Internet. It is not through expropriation of intellectual property rights that new works and technology flourish, but rather through the rights granted to authors and other right holders under copyright law to license and distribute their works on the terms that they see fit. Copyright must be maintained at least at present levels in the networked age. Protection should always be available, but only to those who want to use it. However, protection should not be used as an excuse for censorship.

To facilitate enforcement, the new rights need not result in the diminishment of the benefit of the Internet being a censorship free forum. Copyright and censorship are distinct. There are three classic arguments against extending the ambit of copyright. They are (i) interest in privacy; (ii) interest in freedom of expression; and (iii) transaction costs. Protecting copyright effectively on the Internet does not offend the first two arguments. Transaction costs, that in the sense that they should not be higher than the value of the work itself, are almost negligible in the digital environment and the Internet. In this sense, copyright should in fact protect and reward the labors of the copyright owners. In considering the above arguments, there should always be borne in mind the distinction between free flow information and commercially exploitable content. Often, the choice is one of the author's, as it should be. Rightholders should retain the ultimate decision to determine whether to license their works and enforce their rights collectively or individually.

Procedures and remedies to redress violations of intellectual property protection should be effective, efficient and strong. The principal difficulty in copyright enforcement related to the Internet will be in the legal system, where the procedures can be inadequate, cumbersome

---

[6] See Ejan Mackaay, *The Economics of Emergent Property Rights on the Internet (The Future of Copyright in a Digital Environment)*, 1996, Kluwer Law International (pub)

and slow, and where penalties may be wholly insufficient to redress violations. The cost of proving copyright violation and damages, when compared to the available relief, are a disincentive to the enforcement of authors' and rightholders' rights in even the most obvious of piracy.

Boundaries for new property rights should not be discovered through abstract reasoning. Such boundaries should be drawn from arrangements worked out between interested parties to the transaction, representing at least both sides of the fence. The law should provide the means to build fences with, then individuals could in turn decide for themselves whether they want to use the tools that they are provided with to protect their own interests.

In this regard, the U.S. has extended the distribution right of copyright holders to include the transmission of a work. This is the result of realization that traditional controls on the copying of a work were unlikely to cover its access via the Internet.

If there does not exist a regime capable of protecting effectively the intellectual property rights of individuals, rightowners will start building technical fences, or a combination of technological and contractual provisions, to determine who will have access to the information.

[End of document]