Canadian Journal of Law and Technology

Volume 1 | Number 2 Article 5

4-1-2002

Don't Shoot the Messenger! A Discussion of ISP Liability

Andrew Bernstein

Rima Ramchandani

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/cjlt

 Part of the Computer Law Commons, Intellectual Property Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Andrew Bernstein and Rima Ramchandani, "Don't Shoot the Messenger! A Discussion of ISP Liability" (2002) 1:2 CJLT.

This Article is brought to you for free and open access by the Journals at Schulich Law Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Law Scholars. For more information, please contact hannah.steeves@dal.ca.

Don't Shoot the Messenger! A Discussion of ISP Liability

Andrew Bernstein† and Rima Ramchandani‡

Introduction

In today's world of rampant networked communication, the Internet Service Provider ("ISP") finds itself in a uniquely vulnerable position. As the conduit through which content is disseminated to a numerically and geographically vast audience, the obvious legal risk to ISPs is that those who provide content will do so in a way that attracts legal liability. Like many communications providers (such as publishers or broadcasters), the ISP may have to assume some responsibility for simply providing the means of transmitting content. In some cases, the ISP is more actively involved in the transmission or is knowingly complicit, and the argument for imposing liability may be even stronger. The digital environment itself also raises novel concerns. The ISP makes a very attractive defendant because it is more readily identifiable in the realm of cyberspace where user anonymity is often the norm, because of the jurisdictional problems that arise from the global nature of the Internet, and because the ISP may have deep pockets. Sometimes the ISP is caught in the middle of a dispute between a plaintiff and a pseudonymous defendant, where the ISP is the only legal entity with any information as to the defendant's true identity. The dilemma of the ISP and the legal implications of the role it plays in the networked environment is a highly contentious and currently unresolved area in Canadian law. Given the pervasiveness of online communication, however, it is expected that both the Canadian courts and the legislature will soon be forced to address this issue.

This paper will attempt to describe some potentially troublesome areas for ISPs, and give some suggestions as to how liability can be minimized or avoided. The first part is a discussion of defamation issues, the second part is a discussion of copyright and other intellectual property rights, and the third part addresses the question of liability to subscribers over anonymity issues. We conclude with some contracting tips for ISPs which bolster ISPs' protection beyond the legal regime that is currently in place.

Online Defamation — Liability for Publication of Defamatory Words

United States

Legislation

In the U.S., ISPs are effectively immunized from liability for defamation by third parties by the operation of section 230 of the *Communications Decency Act* ("CDA").[1] As its name suggests, the CDA aims at maintaining standards of decency in cyberspace while encouraging the development and accessibility of new technologies. Further to this goal, the CDA contains a "Good Samaritan" provision stating that providers of interactive computer service (which includes ISPs) are not to be treated as publishers or speakers of information provided by a third party. The original rationale for this protection was to encourage ISPs to develop policies of monitoring and removing offensive content from their servers without fear of being penalized for taking on an editorial role and inviting the liability imposed on "publishers" under the law of defamation. Commentators have noted that while the CDA was enacted to promote decency on the Internet and encourage self-regulation of ISPs, the breadth of the Good Samaritan provision has effectively created a blanket shield from liability for all ISPs, even those that do not monitor their sites.[2] Cases decided before the implementation of the CDA are still cited in the U.S. as courts struggle with the scope of section 230. Moreover, pre-CDA cases may provide assistance to Canadian courts where no such legislation exists or is likely to be enacted.

Caselaw

In *Cubby v. Compuserve*,[3] the District Court of New York granted the defendant ISP's motion for summary judgement in a defamation action. The ISP Compuserve gave its users access to various forums, one of which included a newsletter, *Rumorville*, containing

†Andrew Bernstein is a lawyer in Torys litigation department in Toronto, and a member of Torys' technology group. He will be pursuing his LL.M. at University of California (Berkeley) in 2002-2003.

‡Rima Ramchandani is a student-at-law at Torys.

allegedly defamatory statements about the plaintiff. Compuserve had a contractual relationship with the creator of the forum but had no independent contract with the creator of *Rumorville*. Moreover, Compuserve had no opportunity to review the contents of the newsletter before it was uploaded, it did not compensate the creator of *Rumorville* for the newsletter and it did not receive any fees for access to the newsletter (over and above the general subscription fees charged to all users for access to all services). Before the action was filed, Compuserve was given no notice of the allegedly defamatory statements. The Court held that Compuserve was essentially an electronic library that had little or no editorial control over the contents of these online publications. Compuserve was a distributor, not a publisher, and could not be held liable for distributor liability because it had no knowledge of the defamatory content. The Court stated:

> A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as Compuserve than that which is applied to a public library, book store or news-stand would impose an undue burden on the free flow of information … the appropriate standard of liability to be applied to Compuserve is whether it knew or had reason to know of the allegedly defamatory Rumorville statements.[4]

By contrast, a few years later in *Stratton Oakmont v. Prodigy*,[5] the New York Supreme Court found that the defendant ISP was a publisher and granted the plaintiff's motion for summary judgement against the ISP. *Stratton* involved the anonymous posting of defamatory statements on a bulletin board accessed through Prodigy. The critical issue was whether Prodigy exercised sufficient editorial control over its bulletin boards to render it a publisher with the same responsibilities as a newspaper for filtering content. Prodigy had created an editorial staff of Board Leaders who were responsible for monitoring and censoring bulletin boards according to a set of company guidelines, it had a system of automatic screening in place and it held itself out to the public as controlling the content of its bulletin boards. As such, the Court had little difficulty concluding that Prodigy had brought itself within the definition of a publisher, and was therefore liable.

In response to *Stratton*, Congress enacted the CDA. Section 230 has now become a powerful shield from liability for ISPs. Like *Stratton*, *Zeran v. America Online*[6] involved anonymous postings of defamatory statements on an AOL bulletin board. Upon notification by the plaintiff, AOL removed the original postings but more anonymous postings appeared which were not removed. The Court found that section 230 of the CDA created federal immunity to any cause of action (not simply claims of defamation) that would make service providers liable for information originating with a third party user of the service. Since section 230 precluded courts from treating ISPs as publishers, AOL was protected from liability. The plaintiff argued that AOL was a distributor and that the CDA did not shield ISPs from distributor liability. However, the Court rejected this argument and found that once the ISP received notice of a potentially defamatory posting, it was thrust into the role of a traditional publisher and section 230 prohibited treating the ISP as a publisher.

Following *Zeran,* section 230 has gained considerable force in shielding ISPs from liability. In *Blumenthal v. Drudge and AOL*,[7] AOL escaped liability for defamatory statements made on an online gossip column called the Drudge Report. Even though AOL had paid the author of the report for the right to link to his column and received advance notice of the content of the report, the Court held that section 230 protected it from liability. According to the Court, through section 230, Congress opted not to hold ISPs liable for their failure to edit, withhold or restrict access to offensive material through their services. Although AOL was not a passive conduit like a telephone company, the CDA reflected a legislative policy choice to provide immunity even when ISPs took an aggressive role in making available content provided by others. While the Court acknowledged that AOL had taken advantage of the benefits of the CDA without accepting the burdens of monitoring content, the statutory language was clear and AOL was immune from the suit.[8]

Before the CDA, then, a defamation claim against an ISP for third party content was focused on the extent to which the ISP assumed an editorial function. The enactment of section 230 of the CDA has made this inquiry moot and it appears that all ISPs will be immune from liability regardless of the editorial responsibility they undertake. However, section 230 has its limits. Recently, in *Gucci America v. Hall & Associates,*[9] the defendant ISP was unsuccessful in escaping liability on the basis of section 230 after it was notified that one of its subscribers was infringing the plaintiff's trademarks. The Court looked to the plain language of the CDA and held that it was required to interpret section 230 in a manner that would neither limit nor expand any intellectual property laws. Since this was a case of trademark infringement, section 230 did not immunize the ISP from liability. Despite the breadth of section 230, then, it appears that the U.S. courts will likely only apply it to protect ISPs in claims of online defamation.

A final U.S. case worth noting, in which the editorial role of the ISP was the controlling factor, was *Lunney v. Prodigy.*[10] Although decided after the CDA, the Court in *Lunney* relied on common law principles in excusing Prodigy from liability. *Lunney* also involved the anonymous postings of defamatory messages on a Prodigy bulletin board. Upon becoming aware of the situation, Prodigy removed the offensive postings and closed the accounts of the author. Contrary to the decision in *Blumenthal*, the Court likened Prodigy to a telephone company, a mere conduit which is not expected to monitor the content of its users' conversations. This was a reasonable distinction since the ISP in *Blumenthal* had a con-

tractual relationship with the author of the defamatory statements whereas here, Prodigy had simply provided the forum in which the contents were posted. It followed, then, that Prodigy was not a publisher and could not be held liable. The Court did not go on to consider the potential for distributor liability, presumably because Prodigy removed the postings upon notification of their content. ISPs may therefore be protected from liability at common law as well as under section 230 of the CDA.

United Kingdom

Caselaw from the U.K. will likely be of greater value to Canadian courts since the Canadian common law of defamation tends to follow English rather than American jurisprudence. In the U.K., the essential inquiry for ISP liability has been on whether an ISP can rely on the defence of innocent dissemination. The defence would immunize an ISP from liability if it could show (1) that it is not the author, editor or publisher of the statement; (2) it took reasonable care in relation to its publication; and (3) it did not know, or had reason to believe, that what it did caused or contributed to the publication of the defamatory statement.[11]

The Queen's Bench considered this defence in *Godfrey v. Demon Internet*,[12] and arrived at a conclusion that would make ISPs much more vulnerable to liability for third party content than in the U.S. The facts in *Godfrey* were very similar to those in *Lunney*, involving the anonymous postings of defamatory statements on a newsgroup accessed through Demon Internet. However, unlike Prodigy, Demon Internet did not remove the defamatory postings at the plaintiff's request. The Court held that the transmission of a defamatory posting from the storage of a news server constituted "publication" of that posting to any subscriber who accessed the newsgroup containing that posting. Moreover, the ISP could not claim it was an innocent disseminator because it knew of the defamatory posting and chose not to remove it. Although this was not particularly controversial, what was surprising was the Court's finding that Demon Internet did not play a passive role because it chose to receive and store the newsgroup postings and make them available to users. After reviewing the caselaw from the U.S., Morland J. concluded that the defendant Prodigy in *Lunney* would have been a publisher under U.K. law and would not have escaped liability.

The courts in the U.K., then, apply a much broader concept of publication. It appears that an ISP need not take an active role of editing and/or monitoring in order to invite the title — and responsibility — of publisher. Simply selecting and providing access to particular newsgroups, chat rooms and bulletin boards will be enough to attract liability in the U.K. Of course, had Demon Internet taken swifter action and complied with the plaintiff's request to remove the allegedly defamatory postings, it is possible the Court may have found that it could rely on the innocent dissemination defence. However, given the Court's definition of "publishing", this is not certain.

Canada

As we indicated, to our knowledge there have been no reported Canadian decisions concerning the liability of an ISP for Internet defamation. However, unless the provincial legislatures legislate otherwise (or perhaps Parliament, although it is far from certain that the federal government has sufficient constitutional jurisdiction to legislate in this area), the safe assumption is that the Canadian courts will likely follow some combination of the English and American (pre-*Communications Decency Act*) common law, and decide questions of liability for defamation on the basis of some combination of the following factors:

(a) To what extent did the ISP merely provide access, as opposed to content?

(b) Did the ISP purport to or actually exercise control over the defamatory content?

(c) If it exercised control, did it attempt to screen the contents for defamatory or other offensive content?

(d) Could the ISP reasonably have known about the offensive content?

(e) If it did not make any attempts to screen content in the ordinary course, or could not reasonably be expected to know about the content, was it notified?

(f) If it knew, or was notified, what steps did it take?

Although this is essentially a fair approach, in some ways these principles lead to the one slightly strange result that American legislators were attempting to avoid by enacting section 230 of the CDA: an ISP that completely ignores the content on its network until someone complains is excused from liability, whereas the "Good Samaritan" ISP that takes an active interest in the content may be found liable. The natural consequence is that ISPs will ignore the content on their networks, and investigate only when someone complains. Ironically, section 230 of the CDA does not help, and may even lead to a worse result: by excusing ISPs from liability regardless of whether they review content, not only does the legislation give ISPs an incentive to ignore the content, but also to ignore any complaints, secure in the knowledge that they will not be liable in any event. In any event, unless similar legislation is introduced in Canada (or a province), ISPs should be very cautious if they do decide to exert control over content, and act promptly upon receiving a complaint concerning defamatory postings.

Liability Arising Out of Expectation of Anonymity

Many users consider the Internet to be an anonymous forum. Most posters are able to use a pseudonym, if they are required to post any name at all. Often, the only way to trace a user is by his or her Internet Protocol (IP) address, a set of 4 numbers that is unique to each user at any given time.[13] These IP addresses can be traced back to the ISP, who may be able to then identify its customer from the IP address and the date and time of the posting.[14] Hence, when defamatory or other objectionable statements are posted, it is often the case that the complaining party is only able to obtain, at most, the poster's IP address. In those circumstances, the complaining party will then look to the ISP to provide identifying information.

These requests create a tension for ISPs (as well as other companies that provide access to and services on the Internet). To remain competitive, most ISPs must promise not to disclose information that would reveal their users' identities in their privacy policy or terms of use. Hence, they will rarely do so merely on request. In the civil context, this often results in the plaintiff bringing a motion or application[15] to compel the ISP to reveal the IP address and/or identity of the prospective defendant. In the criminal context, there is no analogous mechanism, so typically the police will obtain a search warrant under the *Criminal Code*.

There are two issues that an ISP must consider when it receives notice of a motion or application. First, the ISP must decide whether to take a position, and if so, what it should be. Most ISPs do not have an interest in maintaining the anonymity of their subscribers. Rather, their interest is in maintaining a good business reputation and minimizing the legal and administrative costs associated with these requests. ISPs that have a clause in their terms of use that state, for example, that they will not reveal their users' identities "except in accordance with a court order or other compulsory process" are in the best position, since they can take the position that they will not participate in the proceeding, but if the court issues an order, they will comply.

ISPs that have an affirmative promise to maintain privacy without this exception are, potentially, in a more difficult position. There is no doubt that they should comply with a court order, if obtained. However, having made this promise to their users, they could easily be criticized for failing to affirmatively oppose the motion or application. In fact, in the United States, Yahoo! was sued by an Internet poster who went by the pseudonym "Aquacool" for complying with what appeared to be a legally valid subpoena. Aquacool's complaints were, essentially, that Yahoo! did not insist on the procedural formalities that would ordinarily be applicable (essentially personal service and acceptance by an in-state court for an out-of-state subpoena), that Yahoo! had promised more privacy protection than it had delivered by acceding to the subpoena, and that Yahoo! had negligently misrepresented its terms of service as it failed to notify him prior to disclosing his identity. Although this suit was ultimately discontinued, it is a reminder to ISPs that they should make a clear statement in their terms of use as to what their position will be when a subscriber's identity is sought by a third party, and then follow it in every case.

The Aquacool case also raises another important issue for ISPs: to what extent should they notify their subscriber of the impending motion or application? While the ISP has no or little interest in maintaining anonymity, the user presumably does. However, it is the ISP, and not the user, who is served with the notice of motion or application. If it does not oppose the order, the truly interested party (the poster) will not be able to defend his or her anonymity until after it has already been lost. Hence, prudent practice suggests that the ISP should advise the user of the pending proceeding, and pass along any materials that have been served. This enables the poster to retain counsel and attend on his or her behalf to argue for maintaining anonymity. Recently, Mr. Justice Spiegel heard such a motion and refused to grant the order requested at that time, adjourning the motion and ordering the Web site in question to serve the three pseudonymous posters with the motion materials and notice of the return of the motion.[16] If other judges follow this practice, it may very well be that both the plaintiff and the ISP will want the subscribers notified in advance of the return of the motion, to ensure that the matter can be resolved with only one court appearance.

One small variation to this scenario is the possibility that, in very serious cases, the plaintiff will want to obtain an *Anton Pillar* order to obtain the defendant's (easily destroyed) computer for evidentiary purposes on an *ex parte* basis. In those cases, ISPs are once again caught between the plaintiff (who has likely repeatedly threatened the ISP with a lawsuit if they fail to cooperate) and the defendant (who is the ISP's customer and who may sue if his or her identity is revealed without notice). In those cases, it would seem that the salutary practice would be to take affirmative pre-litigation action, such as including a clause that the ISP has the contractual right to reveal the subscriber's identity without notice, a good limitation of liability clause, and perhaps even an arbitration clause, which tends to discourage frivolous lawsuits. However, once the litigation has been commenced, the ISP is likely within its rights to take the position that if the plaintiff wishes to keep the order confidential, it is necessary for the judge to so order, and to seal the record under section 137 of the *Courts of Justice Act*. In cases so extreme that an *Anton Pillar* order is sought, it should not be that difficult to obtain such an order, and it relieves the ISP of having to make this determination.

Online Copyright Infringement

In the Internet era, copyright has gone from being an obscure area of the law, familiar to relatively few specialized practitioners and academics, to being a popular conversation topic. Type the word "copyright" into Google (the search engine), and you will find approximately 139,000,000 hits in 0.05 seconds. The fundamental change of the digital age has been the ability to make unlimited copies of text, music, pictures, software and anything else that can be expressed in machine code. Moreover, this can be done essentially anonymously, and by millions of people at the same time. Under these circumstances, it is only natural that those with an interest in preserving the exclusivity that copyright provides (i.e., artists, writers, publishers, etc.) will look to the gatekeepers rather than the individual consumer in an attempt to limit the potential infringements facilitated by digital technology. In this section, we describe the American legislative regime, and in particular the *Digital Millennium Copyright Act*, as well as some caselaw. We then compare this to the Canadian legislative framework which has not been specifically amended to reflect some of the liability issues that may arise. We conclude this section by discussing some proposed legislative changes.

United States

Legislation

In 1998, the U.S. ratified the WIPO treaties through the enactment of the *Digital Millennium Copyright Act* ("DMCA"). Under Title II of the DMCA, online service providers (such as ISPs) can avoid liability if one of its subscribers infringes copyright by following the notice and takedown provisions detailed in the Act. The DMCA contains four "Safe Harbours" of conduct for ISPs: ISPs can limit liability based on (1) transitory communication;[17] (2) system caching;[18] (3) storage of information on systems or networks at direction of user;[19] and (4) information locations tools.[20] To avoid liability, an ISP must not have actual knowledge/awareness of facts indicating that the material is infringing, the ISP must not receive any financial benefit directly attributable to the infringing activity, and upon receiving notification of a claimed infringement, the ISP must expeditiously take down and disable access to the material.[21]

In order to benefit from the limitations on liability in the DMCA, an ISP must designate an agent (with the Copyright Office) to receive notices of infringing activity and must implement a policy of terminating the accounts of subscribers who repeatedly infringe. In short, the DMCA encourages ISPs to be responsible and in return, an ISP is granted immunity from liability. Should an ISP choose not to follow the DMCA provisions, a copyright owner retains the right to seek financial damages from the ISP for contributory or vicarious infringement. As with the law of defamation, then, cases prior to the legislation will still be important in the U.S., and of particular relevance in Canada where no equivalent legislation is in force or being seriously considered.

Caselaw

One of the earlier, and oft-cited, cases of ISP liability for copyright infringement is *Playboy Enterprises v. Frena*.[22] The defendant in *Frena* operated a bulletin board service ("BBS")[23] through which one of his subscribers uploaded infringing copies of Playboy photos. Although the defendant immediately removed the infringing material from his service upon being notified of the matter and began monitoring his service to prevent additional infringement, the Court found the defendant liable for usurping the plaintiff's right to publicly distribute and display its copyrighted work. According to the Court, the lack of intent or knowledge to infringe was not relevant in assessing liability and if anything, the innocence of the defendant would go to the issue of damages.

The case was even stronger for imposing liability on an ISP in *Sega Enterprises v. Maphia*,[24] where the BBS operator solicited subscribers to download copyrighted Sega games onto its service and charged other subscribers a fee to download the games for their personal use. The Court easily found the defendant liable for contributory infringement since it had played an active role in the infringement, providing the facilities for copying, as well as directing and encouraging the copying.

Although the Court in *Frena* did not consider the lack of editorial control by the BBS operator a relevant factor in assessing liability, this was the critical factor in *Religious Technology Center v. Netcom*.[25] Netcom gave its subscribers access to a BBS on which a user had made a series of postings criticizing the Church of Scientology, using the Church's copyrighted materials. The BBS would not remove the postings without proof of the plaintiff's copyright (which the plaintiff was unwilling to give) and Netcom would not disable access to the postings because it could not do so without cutting off all of the other users of the BBS. The Court found that Netcom did not create or control the content of the information available to its subscribers. The Court analogized Netcom to the owner of a copying machine who lets the public make copies but is not responsible for the infringing activities of its customers. An ISP that acts as a mere conduit would not be liable for direct infringement because the necessary element of volition or causation was lacking. Netcom was also not vicariously liable because it did not receive any fees relating to the infringement (aside from its fixed fee to all subscribers for access to all services). However, the Court found that Netcom may be liable for contributory infringement since it had knowledge of the infringing material and ignored the request to remove the postings. The Court speculated that allowing public distribution of infringing material and failing to prevent further damage could

constitute substantial participation in the infringement. Although this was only a motion for summary judgment, the decision clearly indicates that an ISP may be liable as a contributory infringer once it is made aware of the infringement and neglects to rectify the problem.[26]

Frena, *Sega* and *Netcom* were all decided before the DMCA was passed. ISPs that abide by the notice and takedown provisions in the DMCA will now avoid liability for copyright infringement. The germane question is no longer how to deal with the changes in technology, but rather how to interpret the various provisions of the statute.[27]

Canada

The Current Legal Position

At this stage, it is not clear how Canadian courts will address the issue of ISP liability for online copyright infringement.[28] Certainly, the courts in the U.S. have much more extensively considered this issue, and Canada will likely be influenced by many of the policy arguments that pervade those judgments.[29] However, there are differences between the Canadian and U.S. statutes, and, as the Supreme Court of Canada has reminded us, Canadian courts should be wary of merely adopting the American approach.[30]

Under Canada's current copyright regime, ISPs are potentially vulnerable to liability for infringement of telecommunication and reproduction rights. Subsection 3(1) of the *Copyright Act* states:

> 3. (1) For the purposes of this Act, "copyright", in relation to a work, means the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever … and includes the sole right
>
> (a) to produce, reproduce, perform or publish any translation of the work,
>
> (b) in the case of any literary, dramatic, musical or artistic work, to communicate the work to the public by telecommunication
>
> and to authorize any such acts.

"Telecommunication" is defined broadly to include "any transmission of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual, optical or other electromagnetic system".[31]

At first glance, these provisions would appear to catch ISPs. However, the *Copyright Act* contains certain exceptions which appear flexible enough to protect against ISP liability. In particular, ISPs should be able to rely on paragraph 2.4(1)(*b*):

> A person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate the work or other subject-matter to the public.

Just as a letter carrier or a telephone company would be saved from liability by the operation of paragraph 2.4(1)(*b*), so too should the ISP. Of course, the above provisions would only apply to passive ISPs who do not authorize or actively engage in the infringing activity. Thus, an ISP could not escape liability by relying solely on its status as a communications provider and would attract liability should it play a greater role in the infringement.

The potential scope and limits of paragraph 2.4(1)(*b*) as applied to ISPs was recently considered by the Federal Court of Appeal in the judicial review of the Copyright Board's decision in Tariff 22, styled *SOCAN v. Canadian Association of Internet Providers et al.*[32] Tariff 22 is a royalty scheme proposed by Society of Composers, Authors and Publishers of Canada ("SOCAN") for the transmission of musical works over the Internet. Under Tariff 22, the Copyright Board held that ISPs acting as passive intermediaries when communicating musical works to the public by telecommunication will be saved from liability by the common carrier exemption in paragraph 2.4(1)(*b*) of the *Copyright Act*. ISPs cannot benefit from the exemption, however, when they post content, associate with others that offer content, create imbedded links, moderate newsgroups or engage in activities that extend beyond simply providing the means of communication.[33]

The Federal Court of Appeal upheld the Tariff 22 decision in most respects. According to the Court, three conditions must be met in order for paragraph 2.4(1)(*b*) to apply to an ISP: (i) its activities must amount to the *means* of telecommunication; (ii) these means must be *necessary* or enabling another person to communicate a work to the public; and (iii) the activities in question must constitute the ISP's *only act* with respect to the communication.[34] Although the Court recognized that the services provided by ISPs were unlike the more passive physical facilities provided by traditional carriers, it held that the "means of communication" must be interpreted in an expansive way, capable of including technological developments. The Court emphasized that those simply providing the means of telecommunication were passive participants lacking the practical ability to control and monitor content. Importantly, the court appreciated that it is not currently technologically feasible, or at least very expensive and impractical, for ISPs to effectively monitor and prevent the transmission of material. This would, of course, be different when the ISP acts in concert with content providers, and therefore could not benefit from the exception under those circumstances.

While most of the core activities of an ISP are saved by the common carrier exemption, the majority of the Court concluded that caching was not caught by the exemption. Caching enhances the speed of transmission and reduces the cost to the ISP but it is not "necessary" for communication. Hence, caching was not protected by the exemption in paragraph 2.4(1)(*b*), and therefore, to the extent that copyrighted material was being cached, it would constitute an infringement. Justice Sharlow, in dissent on this point, disagreed, stating that

the majority had taken too strict an approach to the definition of "necessary" and that the notion of necessity should include mechanisms for improving the functionality of the means of communication.

The other interesting development with respect to ISPs and copyright that arises out of the Tariff 22 case is SOCAN's argument that when an ISP simply provides customers with an Internet connection, they implicitly authorize the communication of material. However, the Court rejected that argument, finding that since the ISP typically has no contractual or economic relationship with a content provider, they merely facilitate, but do not authorize, communication. Host servers, which store material rather than transmit it to the end user, are in a different position, since they do have a contractual relationship with content providers. This arguably increases the host server's opportunity to monitor and remove material. Nonetheless, the Court held that host servers merely facilitate the communication of material by supplying equipment that enables others to communicate. Host servers, then, are also passive participants and can not be said to authorize communication. The Court did suggest, however, that a contractual term prohibiting the posting of infringing material, although not determinative, would help make it clear that the operator does not sanction the communication. Finally, the Court found that implicit authorization may be inferred if host servers neglected to remove infringing material once notified of its existence.

The rationale behind the common carrier exemption under the *Copyright Act* is similar to the innocent dissemination defence for the common law of defamation — a person who transmits information without (ordinarily) having any capacity to control the information transmitted ought not to be held civilly liable for someone else's use of their transmission facilities. However, when the transmitter takes on some other role, they are no longer entitled to the benefit of that protection.

Although there have been no Canadian decisions holding an ISP liable for copyright infringement in the civil courts, a bulletin board operator was convicted criminally under the *Copyright Act*. In *R. v. M. (J.P.)*,[35] the accused was a 17-year-old operator of a computer bulletin board which allowed users to download copyright protected software programs. The accused played a very active role in the infringement, uploading the copyrighted material, providing access to users, and even supplying the software required to copy the programs. The Nova Scotia Court of Appeal found that the accused's actions were an infringement of the right of telecommunication and further, that in controlling the means and manner by which the users of the BBS accessed and downloaded the material, the operator was also criminally liable for "distributing" the infringing material. Although the Court did not discuss the operation of paragraph 2.4(1)(*b*) presumably the accused could not have benefited from the intermediary exception given his active involvement in the infringing activity.

Public Policy Development

The Consultation Paper issued by Industry Canada and Canadian Heritage provides some further indication of the way in which the issue of ISP liability for online copyright infringement may unfold.[36] The paper outlines a proposal which would include a limited role for government regulation to establish copyright liability rules that are clear and fair. The paper raises the possibility of establishing a complaints-driven notice and takedown process similar to the DMCA that would address the concerns of both rights-holders and ISPs. Importantly, an ISP that blocks access to an allegedly infringing site in good faith would not be liable for the harm suffered in consequence of this action. However, the paper acknowledges the concerns about a notice and takedown regime, specifically that such a system would represent a considerable overhead expense for ISPs and that it may discourage ISPs from participating in voluntary licensing-based initiatives from the online environment.

The Canadian Association of Internet Providers ("CAIP"), a private organization whose current members provide more than 85 per cent of the Internet connections to Canadian homes, schools, and businesses, has (perhaps not surprisingly) responded to the Consultation Paper with comments that argue for greater self-regulation. CAIP dislikes the "drastic and potentially legally contentious action by an ISP of actively taking targeted content down without a court order."[37] Instead, it proposes a "Notice and Notice" regime where copyright holders alleging infringement would issue statutory-defined notice to an ISP and ISPs, in turn, would provide a statutory-defined notice of the allegation to the party responsible for the alleged infringement. Should this process not result in the voluntary removal of the allegedly infringing content, CAIP argues an ISP should only be required to take down the content when served with a court order. According to CAIP, "requiring ISPs to take down content based solely on the allegations of a third party, would run counter to the fundamental principle of Canadian law that someone is innocent until proven guilty".[38]

In our view, the real issue behind this debate is the "default" position and, conversely, who is required to go to court to preserve their preferred outcome. A notice and take-down regime ensures that potentially infringing materials are immediately removed from the Web site (since most ISPs are indifferent as to whether the material stays or is removed, but will remove it to ensure they suffer no liability). Hence, it is the party who posted the allegedly infringing material that will have to seek a court order to reinstate it. Conversely, a notice and notice regime, since it does not require the ISP to remove the material to escape liability, places the onus on the

copyright owner to seek a court order. If litigation were costless and instantaneous, which regime is selected should not particularly matter. However, since the reality is quite the opposite, the time and expense of seeking a court order means that the default position will likely prevail in the overwhelming number of cases.

There is no obvious solution to this debate. On the one hand, we find the "innocent until proven guilty" argument in support of notice and notice thoroughly unpersuasive. The consequences (removal of the offending materials) are much less than a criminal sanction, and copyright owners regularly obtain interlocutory injunctions merely by demonstrating a *prima facie* case. On the other hand, the notice and take-down regime effectively reverses the ordinary situation, in which the copyright holder is required to seek the court's protection by showing there has been a violation of copyright, and the alleged infringer is not required to seek the court's permission by showing there is not. If this is to be reversed for the Internet, copyright holders should clearly articulate a reason, such as (perhaps) the detrimental effects that digital technology has had on their ability to protect their works.

Conclusion and Pre-Litigation Practice

Although the legal consequences of owning and operating an ISP have yet to be considered in Canada, we have the benefit of examining the two contrasting approaches to ISP liability taken by the U.S. and the U.K. When faced with a seemingly novel legal issue, some jurisdictions (such as the U.S.) respond with an arsenal of legislation to combat the problem, while others (such as Canada and the U.K.) tend towards adapting existing laws. Despite the difference in approach, however, the end result is surprisingly not that dissimilar. All three jurisdictions endorse responsible conduct on the part of an ISP and reward this responsibility with limited liability. Although the CDA is a powerful shield for ISPs charged with online defamation, an ISP will also be protected in the U.K. (and likely Canada) if it meets the requirements for innocent dissemination. Likewise, the notice and takedown provisions of the DMCA also encourage ISPs to be alert and responsive to online infringement. The lesson for ISPs is that the likelihood of liability is significantly reduced if they take some reasonable precautions and conduct themselves responsibly. We end this paper with some (perhaps obvious) tips for ISPs that can help them avoid litigation or liability:[39]

- An ISP should ensure that the terms and conditions of its subscription contracts clearly indicate that users are not to make illegal or civilly unlawful use of their access.
- An ISP should institute and implement an "Authorized Use" policy and such policy should include a contact name within the organization for customers who experience problems; the policy should be communicated to subscribers and the general public, and should be periodically reviewed and updated.
- An ISP should implement a "Privacy Policy" that clearly articulates the extent of the protection offered, and not offered, to its subscribers. In particular, it should not make unqualified promises to its subscribers that their privacy and/or personal information will be protected and/or remain confidential; such terms should be tempered with words such as "unless we believe it to be required by law" or "subject to legal process or compulsion".
- An ISP should have a system in place to quickly remove obscene, infringing or defamatory content from its servers, and the terms of this regime should be clearly communicated to subscribers.
- An ISP should consider configuring its network to bar access to sites that are known as defamatory, illegal, obscene or infringing.
- An ISP should specify the appropriate jurisdiction in the event of a legal dispute.
- An ISP's user agreement should have a good limitation of liability, that includes the following elements:
  - a clause that strictly limits liability to a subscriber to the cost of the service;
  - an indemnity obliging the subscriber to indemnify the ISP for any content posted;
  - an arbitration clause to attempt to avoid class proceedings; and
  - for ISPs servicing the consumer, a representation and warranty by the user that the service will be used for personal use only, and not for business use.

Notes:

[1] 47 U.S.C. § 230.

[2] M. Deturbide, "Liability of Internet Service Providers for Defamation in the U.S. and Britain: Same Competing Interests, Different Responses", 2000 (3) online: The Journal of Information, Law and Technology <http://elj.warwick.ac.uk/jilt/00-3/deturbide.html> (date accessed May 30, 2002).

[3] 776 F. Supp. 135 (S.D.N.Y. 1991) [hereinafter *Cubby*].

[4] *Ibid.* at 140.

[5] 23 Media L. Rep. [hereinafter *Stratton*].

[6] 129 F. 3d 327 [hereinafter *Zeran*].

[7] 992 F. Supp. 44 [hereinafter *Blumenthal*].

[8] See also *Jane Doe v. America Online*, 783 So. 2d 1010 (Fla. Sup. Ct. 2001) where section 230 was used to shield AOL from liability in a negligence claim for failing to monitor the marketing of pornographic pictures and videos in one of its chat rooms. In dissent, Lewis J. held that section 230 was not designed to totally exonerate and insulate an ISP from responsibility particularly where the ISP has acted as a knowing distributor of illegal material. The majority interpretation, according to Lewis J., "transformed [section 230] from an appropriate shield into a sword of harm" and undermined the intent of the CDA. As of the date of this paper, Lewis's dissenting opinion has not yet been followed. See also *Jane Doe v. Shannon Oliver*, 46 Conn. Supp. 406 (Conn. Sup. Ct. 2000) where the Court struck complaints of negligence against AOL for its failure to prevent the transmission of offensive e-mail on the basis of section 230.

[9] 135 F. Supp. 2d 409 (N.Y. Dist. Ct. 2001).

[10] 94 N.Y. 2d 242 (N.Y. Ct. App. 1999) [hereinafter *Lunney*].

[11] *Defamation Act 1996*, c. 31 s. 1(1). The Act (and its defence of innocent dissemination) is essentially a codification of common law principles.

[12] E.W.J. No. 7345 [hereinafter *Godfrey*].

[13] The IP address is the addressing system for the Internet. When a user types "www.google.com" into a browser, the browser first contacts the registrar to determine the IP address for google.com, and then tells the user's computer to go to that address.

[14] Whereas some ISPs still assign static IP addresses (i.e., a user retains his or her IP address for a certain period of time), most now use dynamic IP addresses (where a user is assigned a new IP address every time he or she goes online).

[15] Although the appropriate procedure is not really apparent from the *Ontario Rules of Civil Procedure*, it seems to us that it is best brought as a motion for third party discovery of the sort Justice Wilkins ruled on in *Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318.

[16] *Dimethaid Research Inc. et al. v. John Doe #1 et al.*, Court File No. 01-CV-221269CM2, January 2, 2002, per Spiegel J.

[17] This provision is aimed at providers that are mere data conduits transmitting digital information from one point on a network to another at someone else's request. This limitation covers acts of transmission, routing, or providing connections for information, as well as the intermediate and transit copies that are made automatically in the operation of a network. U.S. Copyright Office, "The Digital Millennium Copyright Act of 1998; Digital Millennium Copyright Act Study", online: U.S. Copyright Office <http://www.copyright.gov/reports/studies/dmca/dmca_study.html> (date accessed: May 28, 2002).

[18] This provision limits the liability of a provider for the practice of retaining copies, for a limited time, of material that has been created online by a third party and then submitted to a subscriber at his/her direction. *Ibid.*

[19] This provision limits the liability of a provider for copyright infringing materials on a Web site hosted on the provider's server. *Ibid.*

[20] This provision limits the liability of a provider for referring users to a site containing infringing material through information location tools such as hyperlinks, online directories and search engines. *Ibid.*

[21] *Ibid.*

[22] 839 F. Supp. 1552 (M.D. Fla. 1993) [hereinafter *Frena*].

[23] Bulletin board services were essentially the equivalent of ISPs in the early days of the Internet.

[24] 857 F. Supp. 679 (N.D. Calif. 1994) [hereinafter *Sega*].

[25] 907 F. Supp. 1361 (N.D. Calif. 1995) [hereinafter *Netcom*].

[26] This reasoning is consistent with *Godfrey* where the Court suggested that the ISP could have benefited from the defence of innocent dissemination had it acted more responsibly once it was notified of the defamatory postings.

[27] In *Als Scan v. Remarq Communities*, 239 F. 3d 619 (4th Cir. 2001), for example, the Court considered the notice requirements under the DMCA and held that substantial compliance with the notice requirements was sufficient to trigger the takedown obligations. Although the plaintiff had not provided a "representative list" of the infringing material, as required by the Act, the Court found that its letter indicating the two sites on which all of their copyrighted works could be found met with the requirements under the Act. This case suggests that the courts will be fairly lax in interpreting the notice requirements under the DMCA and that ISPs will not be able to evade their obligations under the Act by relying on technical arguments of non-compliance.

[28] An additional consideration, outside the scope of this paper, is the applicability of foreign legislation such as the DMCA to Canadian ISPs. According to the WIPO "private international law attributes jurisdiction to national courts when disputes involve a foreign element, determines the applicable law, and facilitates recognition and enforcement of foreign judgements. It does so on the basis of connecting factors, such as the domicile of a person, the place of registration … the place of infringement." "WIPO Forum on Private International Law and Intellectual Property" online: World Intellectual Property Organization http://www.wipo.org (site modified daily). See also *Braintech v. Kostiuk*, [1999] B.C.J. No. 622, where the B.C. Court of Appeal recently refused to enforce a Texas default judgment against a B.C. resident found liable for posting defamatory content on the Internet. The Court disagreed with Texas taking jurisdiction since there was no evidence that anyone in Texas had ever viewed the defamatory posting. Although not a case about ISP liability, the decision suggests that U.S. judgments (based on U.S. legislation such as the DMCA or the CDA) will not be enforced by Canadian courts absent sufficient connecting factors to the U.S. jurisdiction. Conversely, Canadian ISPs may benefit (or suffer) from exposure to liability in the U.S., based on U.S. legislation such as the CDA and DMCA, should there exist sufficient connecting factors for the U.S. courts to take jurisdiction.

[29] In *Robertson v. Thomson*, [2001] O.J. No. 3868 which was not a case about ISP liability, Cumming J. indicated that it is important to take account of the differences in the respective statutes, but that where the policy rationales are similar, it is appropriate to apply U.S. law.

[30] *Compo v. Blue Crest Music*, [1980] 1 S.C.R. 357.

[31] *Copyright Act*, R.S.C. 1985, c. C-42, s. 2.

[32] (2002) FCA 166 [hereinafter *SOCAN v. CAIP*].

[33] Statement of Royalties to be Collected for the Performance or the Communication by Telecommunication, in Canada, of Musical or Dramatico-Musical Works (Tariff 22 — Transmission of Musical Works to Subscribers Via a Telecommunications Service Not Covered Under Tariff Nos. 16 or 17), [1999] C.B.D. No. 5 at p. 41, online: QL (CBD).

[34] *Supra* note 32.

[35] 67 C.P.R. (3d) 152.

[36] "Consultation Paper on Digital Copyright Issues", online: Industry Canada <http://strategis.ic.gc.ca/SSG/rp01099e.html> (site modified daily).

[37] "Re: Consultation Paper on Digital Copyright Issues", online: The Canadian Association of Internet Providers <http://www.caip.ca/issueset.htm> (site modified daily).

[38] *Ibid.*

[39] Many of these suggestions were taken from the Joint Information Systems Committee Web site at http://www.jisc.ac.uk/legal/ISP liability.html and from the Canadian Internet Service Providers Fair Practices Manual at http://www.caip.ca/issues/images/FairPractices-p.pdf.