

COPYRIGHT INFRINGEMENT IN THE INTERNET ERA: THE CHALLENGE OF MP3S

ALEX COLANGELO*

The advent of new technologies, such as the digitization of music and Internet networking, has greatly expanded the ease with which copyright infringement can occur. These new technologies have made it possible for the average computer user to bypass copyright laws effortlessly and without detection, at a substantial cost for legitimate copyright holders. It will be argued in this article that stronger domestic legislation is needed in order to adequately protect copyright owners from widespread infringement.

L'avènement de nouvelles technologies telles que la numérisation de la musique et le réseautage par Internet a considérablement facilité la violation des droits d'auteurs. Grâce à ces nouvelles technologies, il est possible pour un usager ordinaire d'un ordinateur d'éviter les droits d'auteurs facilement et sans être décelé, ce qui représente des coûts importants pour les détenteurs de ces droits d'auteurs. Cet article fait valoir l'importance d'une loi nationale plus rigoureuse afin de protéger adéquatement les détenteurs de droits d'auteurs de ces violations généralisées.

TABLE OF CONTENTS

| | | |
|------|---|-----|
| I. | INTRODUCTION | 892 |
| II. | ON-LINE TECHNOLOGIES | 892 |
| | A. THE INTERNET | 892 |
| | B. MP3 | 894 |
| III. | LEGAL EFFORTS IN THE UNITED STATES AND INTERNATIONALLY | 895 |
| | A. EFFORTS IN THE UNITED STATES | 895 |
| | B. WIPO | 900 |
| | C. INTERNATIONAL EFFORTS | 901 |
| IV. | CANADIAN PROTECTION | 902 |
| | A. COPYRIGHT LAW IN CANADA | 902 |
| | B. CANADA'S OBLIGATIONS UNDER THE <i>WIPO COPYRIGHT TREATY</i> | 903 |
| V. | OTHER SOURCES OF PROTECTION | 905 |
| | A. SECURE DIGITAL MUSIC INITIATIVE | 905 |
| | B. BLANKET ROYALTY SCHEMES | 907 |
| VI. | ISP LIABILITY | 908 |
| | A. INTERNATIONAL EFFORTS ON ISP LIABILITY | 909 |
| | B. CANADIAN EFFORTS ON ISP LIABILITY | 910 |
| VII. | CONCLUSION | 912 |

* LL.B. 2001 (University of Western Ontario), LL.M. Candidate 2002 (University of Ottawa). The author would like to thank Professor Margaret Ann Wilkinson of the University of Western Ontario and Professor Daniel Gervais of the University of Ottawa for their comments and suggestions with regard to this article.

I. INTRODUCTION

Intellectual works have been protected by law in Canada from unauthorized reproduction and distribution, except under certain circumstances, since before confederation.¹ While piracy in copyright works has been a problem for years, the advent of new technologies has greatly expanded the ease with which copyright infringement can occur. Computer software has made it easy to copy songs from a CD to a format known as MP3,² while the Internet has made the distribution of these works easy and inexpensive. Technology such as Napster³ allows Internet users to share MP3 files online by creating a network of computers over the Internet. These new technologies have made it possible for the average computer user to bypass copyright laws effortlessly and without detection, at a substantial cost for legitimate copyright holders.

This article will outline the legal issues related to these new technologies and possible legal solutions. First, the nature of the Internet and on-line technologies will be examined. Second, the legal efforts made in the United States and other international jurisdictions, including adherence to the *World Intellectual Property Organization Copyright Treaty* ("WIPO")⁴ will be considered. Third, relevant Canadian copyright law will be examined. It will subsequently be argued that stronger domestic legislation is needed in order to adhere to our WIPO obligations and adequately protect copyright owners from widespread infringement.

II. ON-LINE TECHNOLOGIES

A. THE INTERNET

The predecessor of the Internet, the ARPAnet, was developed by the US Department of Defense's Advance Research Project Administration ("ARPA") and debuted in 1969.⁵ Originally consisting of a network of four computers, the ARPAnet's purpose was to provide military researchers with a decentralized computer network able to withstand a Soviet nuclear attack.⁶ The network employed a method of information transmission dubbed "packet-switching" that divided transmissions into separate pieces of data called "packets," which were each assigned the address of their final destination.⁷ The packets would then be sent independently through the network using the fastest available route and would be reassembled at the final destination.⁸ This allowed the transmission of data to continue even if a computer on the network failed, as the packets would simply travel

¹ See D. Vaver, *Copyright Law* (Toronto: Irwin Law, 2000).

² See Part II.B., below, for an explanation of the nature of MP3s.

³ See Part III.A.4., below, for an explanation of Napster technology.

⁴ See *infra* note 70 and accompanying text for more on the *WIPO Copyright Treaty*.

⁵ A. Staiman, "Shielding Internet Users From Undesirable Content: The Advantages Of A PICS Based Rating System" 20 *Fordham Int'l L.J.* 866.

⁶ A. Terett, "A Lawyers Introduction to the Internet," online: University of Edinburgh School of Law <www.law.ed.ac.uk/it-terr1.htm> (date accessed: 3 December 2000). See also Staiman, *supra* note 5. The following description of the history of the Internet will be given from these sources.

⁷ Terett, *ibid.*

⁸ *Ibid.*

through an alternate path. The ARPAnet was soon embraced by military researchers and university scientists who realized that it was a useful and efficient communication tool.

A major development with respect to the Internet occurred in 1989 when researchers at CERN, the European Physics Particle Laboratory, developed the Hypertext Transfer Protocol (“HTTP”).⁹ HTTP allows different types of content to be displayed on a single web page. A further development occurred with the creation of Hypertext Markup Language (“HTML”).¹⁰ HTML standardized the programming of web pages, which led to the development of Internet “browsers” that were able to “surf” and graphically display web pages.

The popularity of the “World Wide Web” multiplied for three main reasons.¹¹ First, the World Wide Web can distinguish between various file types such as text and images. Second, it allows for hypertext links that link web pages with one another, making it simple for users to navigate between web pages. Third, the World Wide Web employs a Graphic User Interface, which makes the World Wide Web accessible for the average computer user who does not understand the fundamentals of computer language.

These developments led to an explosion of resources dedicated to the Internet as usage expanded. In its infancy in 1993, there were only about 50 servers dedicated to the World Wide Web.¹² By 1997 there were over 100,000.¹³ As the commercial potential of the Internet became obvious, the World Wide Web and the Internet developed into a medium used by businesses and the general public in a variety of ways. Search engines have made finding and retrieving information quick and easy. Making information available to Internet users is also inexpensive as many Internet Service Providers (“ISPs”) offer a fixed amount of free space on their servers for customers to establish their own presence on the web.¹⁴ Internet users can also utilize commercial sites like “Yahoo! Geocities” and “Tripod.com,” which offer free space to host a personal web site in return for hosting advertisements on the page.¹⁵ This allows the average Internet user to create a web site and provide information and files of any type to users around the world, provided they stay within their spatial limit as dictated by the service providing the hard disk space.

The ease with which a person can now offer information over the Internet creates complex challenges for the owners of intellectual property. A user can easily create a web page that displays the contents of a book, which is copyrighted in its entirety or that displays a trademark, using very little file space. Detecting such acts and forcing the

⁹ *Ibid.*

¹⁰ *Ibid.*

¹¹ *Ibid.*

¹² Staiman, *supra* note 5 at 874.

¹³ *Ibid.*

¹⁴ See “Rogers@Home, Advantages,” online: Rogers Communications Inc. <rogers.home.com/AdvantagesIndex.html> (date accessed: 3 December 2000), which describes the advantages of using Rogers as an ISP, including 5 Meg of personal webspace free with service.

¹⁵ See, e.g., “Membership Brochure,” online: Yahoo! GeoCities <www.geocities.com/join_info.html> (date accessed: 3 December 2000), which describes the advantages of maintaining a web site on “Yahoo! Geocities” including 15 Meg of personal webspace free.

removal of material can be onerous as the computer on which the files reside could be in one country, while the person who posted the material could be residing elsewhere. The anonymity of the Internet also makes it difficult to find the person responsible for such acts. While music files have traditionally been excluded from such piracy because of the sheer size necessary to copy a single song into a digital format, the advent of MP3 technology has drastically reduced the amount of space required to digitize a music selection. Whereas the resources necessary for music piracy previously made it impractical, users can now easily post or transmit pirated sound recordings over the Internet.

B. MP3

While copyright infringement has always been a problem, hardware technology available in the past had a limiting effect. Music stored on compact discs could be duplicated onto a computer, but the sheer size of the file would inhibit the popularity of digitizing songs. The size of the files would also prohibit users from sharing these files with other computer users since floppy disks did not have the capacity to hold the full-length music files, and the time needed to transmit a file over the Internet was extremely lengthy. A new audio format, however, addresses these concerns.

This new technological advance, which threatens to undermine copyright law, is the new digital music format: Motion Picture Experts Group Audio Layer 3 or MP3.¹⁶ Unlike music on cassettes or CDs, MP3s are completely digital and are not bound to any physical medium. MP3s employ a method of file compression called "perceptual audio coding" methods.¹⁷ By stripping away digital information inaudible to the human ear from the sound recording, much of the sound data can be discarded from the digitized file. This allows very large music files to be digitized in minimal amounts of space. The result is a file that challenges CDs for quality but that is comparatively much smaller than an uncompressed file.¹⁸ The rate of file compression is typically between 10:1 and 12:1.¹⁹ As these files are a fraction of the size of a regular CD file, the compact disc is no longer necessary as a storage device for music.

The expansion of the average sized hard drive along with the decreasing prices of memory storage has made it economically practical to store vast numbers of music files on one's personal computer for later listening. Whereas an uncompressed music file required approximately 50 megabytes of hard disk space, the typical MP3 is less than 5 megabytes in size.²⁰ While an uncompressed music file could take two hours to download or transfer to another user on the Internet using a 56 kbs. modem, a compressed MP3 can be downloaded in about 5 minutes.²¹

¹⁶ See "MPEG Audio Layer-3," online: Fraunhofer Institute for Integrated Circuits <iis.fhg.de/amm/techinf/layer3/index.html> (date accessed: 4 November 2001).

¹⁷ *Ibid.*

¹⁸ *Ibid.*

¹⁹ *Ibid.*

²⁰ J. Selby, "The Legal and Economic Implications of the Digital Distribution of Music: Part I" (2000) 11:1 Ent. L. Rev. 4 at 6.

²¹ *Ibid.*

The advent of MP3s and file sharing technologies has completely changed the Internet music environment. The small size of MP3s and the file sharing technology available makes it easy and inexpensive for users to seek and copy digital music over the Internet. Compression technology coupled with the advance in modem speeds and the fast expansion of the Internet has made the sharing of MP3s a problem unforeseen in the past.

III. LEGAL EFFORTS IN THE UNITED STATES AND INTERNATIONALLY

A. EFFORTS IN THE UNITED STATES

American efforts have undoubtedly been shaped by the demands of the recording industry. Worldwide, the music industry is worth almost \$40 billion (US) a year.²² The United States accounts for 37 percent of world sales, while Canada accounts for 2.3 percent of that total.²³ Canada's total, therefore, is approximately \$920 million (US). Music artists are usually awarded royalties of between 11 percent and 15 percent.²⁴ The Recording Industry Association of America ("RIAA") estimates that \$4.5 billion (US) is lost annually to music piracy worldwide.²⁵ Undoubtedly, the recording industry and music artists have much at stake in protecting their copyright interests.

Article I, s. 8 of the Constitution of the United States assigns the power to make laws with respect to copyright to the federal Congress.²⁶ The original American *Copyright Act* of 1790 only protected the musical composition itself and did not extend to any physical sound recording or to the performance of the musical composition.²⁷ With the passing of the *Sound Recording Act*²⁸ of 1972, Congress extended copyright protection to sound recordings and incorporated this protection into the *Copyright Act* of 1976.²⁹ Rights in performances were enacted in 1992 with the passage of the *Audio Home Recording Act*.³⁰ With respect to digital music, the United States Congress passed the *Digital Performance Right in Sound Recordings Act of 1995*,³¹ and the *Digital Millennium Copyright Act*³² in 1998 to protect copyright in digital works transmitted over the Internet.³³

²² See "The World Sound Recording Market," online: RIAA <www.riaa.com/MD-World.cfm> (date accessed: 19 October 2001).

²³ *Ibid.*

²⁴ B.M. Schulman, "Song Heard 'Round the World': The Copyright of MP3s and the Future of Digital Music" (1998-99) 12 *Harv. J. L. & Tech.* 589 at 599.

²⁵ "Effects," online: RIAA <www.riaa.com/Protect-Campaign-3.cfm> (date accessed: 19 October 2001).

²⁶ Ch. 15, 1 Stat. 124 (1790) (repealed 1831). See also *supra* note 20.

²⁷ See Schulman, *supra* note 24 at 602-603.

²⁸ 17 U.S.C. § 102 (1994 & Supp. III 1997).

²⁹ 17 U.S.C. § 102 (1994 & Supp. III 1997) (renumbered Chapter 17; enforced starting in 1978). See also Schulman, *supra* note 24 at 602-603.

³⁰ Pub. L. No. 102-563, 106 Stat. 4237 (1992). See also Schulman, *ibid.* 17 U.S.C. §§ 1001-1010.

³¹ Pub. L. No. 104-39, 109 Stat. 336.

³² Pub. L. No. 105-304, 112 Stat. 2860 (1998).

³³ See Schulman, *supra* note 24 at 602-603 for a discussion of chronology of the passage of these statutes and their significance with respect to rights.

I. UNITED STATES *AUDIO HOME RECORDING ACT*

The *Audio Home Recording Act* has its roots in the case of *Sony Corp of America v. Universal City Studios, Inc.*³⁴ The case concerned the Betamax videocassette recorder, which Universal City Studios claimed would increase the amount of pirating of television programs and movies and thus copyright infringement. The plaintiffs claimed that Sony was, therefore, liable for contributory copyright infringement in producing the product.³⁵

The United States Supreme Court relied on the "fair use" doctrine in this case, accepting that the videocassette recorder was primarily used to record television programs for later viewing. This "time shifting" use was found to be a fair use and subsequently, no copyright infringement was found.³⁶

A perceived direct threat to the music industry surfaced with the introduction of the Digital Audio Tape ("DAT") machine in the late 1980s.³⁷ Unlike the Betamax machine, a DAT device was able to create reproductions of copyright material with no real reduction in sound quality.³⁸ Another difference between the DAT device and a VCR is that unlike television programs which, once taped, are usually viewed only once, music is usually kept for a longer time, allowing individuals to build personal libraries of music, which they can listen to time and time again.³⁹ This threatened to damage the recording industry substantially as copies of musical works would displace the need to purchase the sound recording legitimately. The recording industry, through an appropriate plaintiff, began pursuing litigation for copyright infringement.⁴⁰ Negotiations between the parties led to a framework agreement, which the United States Congress introduced as legislation, and which eventually became the *Audio Home Recording Act* of 1992.⁴¹

The *AHRA* sought to prevent the widespread infringement of copyrighted sound recordings. The *AHRA* attempted to achieve this by creating a legislative scheme that took into account the available technologies. The *AHRA* required that all digital audio recording devices be equipped with a Serial Copy Management System ("SCMS"), which would only allow a copy of a sound recording to be made from the original recording. This SCMS is achieved by an encoding on the original sound recordings. Subsequent copies would lack the encrypted code, making third generation copying impossible. While this still allowed users to make limitless copies of an original, it was hoped by Congress that the *AHRA* would achieve an acceptable balance between precluding the ability to make third and fourth generation copies and allowing a legitimate user to make a personal copy for personal use.

³⁴ 464 U.S. 417 (1984) [hereinafter *Sony*].

³⁵ Schulman, *supra* note 24 at 605.

³⁶ R.J. Hill, "Pirates of the 21st Century: The Threat and Promise of Digital Audio Technology on the Internet" (2000) 16 *Computer & High Tech. L.J.* 311 at 324.

³⁷ Schulman, *supra* note 24 at 606.

³⁸ *Ibid.*

³⁹ *Ibid.*

⁴⁰ See *Cahn v. Sony Corp.* (9 July 1990), No. 90-4537 (S.D.N.Y.).

⁴¹ *Supra* note 30 [hereinafter *AHRA*]. See also Schulman, *supra* note 24 at 607.

A SCMS, however, would not completely preclude the pirating of sound recordings as experience has shown that technological measures protecting copyright are never foolproof.⁴² To this effect, the *AHRA* also mandated that royalties be paid for every digital audio recording device sold in order to offset the economic costs of piracy. In return for implementing a SCMS and paying a blanket royalty, the *AHRA* provided broad immunity for manufacturers of digital audio recordings from liability for contributory infringement.

2. *RIAA v. DIAMOND*⁴³

A test of the boundaries of the *AHRA* occurred in 1998 when the RIAA filed suit against Diamond Multimedia over the production of its "Rio" MP3 player.⁴⁴ The Rio is a Walkman sized unit capable of receiving MP3 music from a computer and storing it for playback through headphones. The portable unit can store approximately thirty minutes of music and can be taken anywhere, much like a Walkman. The RIAA claimed that the Rio player would encourage the widespread pirating of digital music as it removed the use of MP3 from the exclusive domain of computers and the Internet and into wider portable use.

Ultimately, the Court found that the Diamond Rio did not fall within the domain of the *AHRA* as it could not download or transmit the files to another device and thus lacked recording capabilities.⁴⁵ While the ruling confirmed the status of units with only playback capabilities, future units with recording capabilities can be envisioned. As these will fall under the *AHRA*, they will be required to have a SCMS as part of the unit, and a blanket royalty will apply to the sale of each unit.

3. *DIGITAL MILLENNIUM COPYRIGHT ACT*

In order to increase protection for copyright works online, the United States passed the *Digital Millennium Copyright Act* in October of 1998.⁴⁶ The *Act* attempts to protect copyright material online by prohibiting the production or sale of devices designed to evade the technological measures that protect on-line materials.⁴⁷ An example would be a device that could make copies of digital audio recordings by bypassing the SCMS mandated by the *AHRA*. Software that could defeat the encryption on copyright material and allow access to copies would also be prohibited.

The *DMCA* also provides protection from liability for copyright infringement for ISPs. For most Internet users, an ISP is the link that provides access to the Internet. A user

⁴² See, e.g., 111 F. Supp.2d 294 (N.Y. Dist. Ct. 2000) a case involving a Norwegian teenager who was able to create a software program able to circumvent the encryption measures used by motion picture studios to protect digital videos from unauthorized copying.

⁴³ *Recording Industry Association of America v. Diamond Multimedia Systems, Inc.*, 29 F. Supp.2d 624 at 632-33 (Cal. Dist. Ct. 1998), aff'd 180 F.3d 1072 (9th Cir. App. 1999).

⁴⁴ Hill, *supra* note 36 at 332.

⁴⁵ *Supra* note 43. See also *ibid.* at 333-34.

⁴⁶ *Supra* note 32 [hereinafter *DMCA*]. See Hill, *supra* note 36 at 326.

⁴⁷ Hill, *ibid.* at 326-29.

simply connects to the ISP server, which acts as a gateway to the Internet. Under the *DMCA*, ISPs would be protected from liability for copyright infringement where the ISP is merely a conduit for the transmission of copyright materials.⁴⁸ ISPs would have a duty, however, to address infringement issues by, for example, taking steps to “take down” infringing material in return for a “safe harbor” defence under the *Act*.⁴⁹

4. *A & M RECORDS V. NAPSTER*⁵⁰

Napster is a software program developed to allow users to share music files over the Internet.⁵¹ The Napster web site does not actually host any of the MP3 music files that users download, using instead “peer-to-peer” technology to act as a conduit for users to connect to other users.⁵² Napster maintains a central server to coordinate user profiles. When a user searches for a particular song, the software links the user with other users who have that particular song present on their computers. The user searching for the song can then begin downloading the song directly from the other user’s computer. Napster does not actually house any music files itself. It only maintains a central database of users. Therefore, the Napster server does not actually copy or make available any copyrighted works.⁵³

While the RIAA was unable to stop the production of portable MP3 players, the RIAA has firmly set its sights on on-line services such as Napster, which threaten to undermine copyright protections worldwide. On December 6, 1999, the RIAA filed suit against Napster, claiming that the company was liable for contributory and vicarious copyright infringement.⁵⁴ Contributory infringement occurs under American law when the party has knowledge that copyright material is being pirated and subsequently contributes to the infringing activity.⁵⁵ Vicarious copyright infringement occurs when the party has control over the infringing acts and financially benefits from such acts.⁵⁶

One of the arguments put forward by Napster in its defence was that it acted merely as a conduit for copyright material and was, therefore, protected from liability by the *DMCA*.⁵⁷ The Court rejected this argument for two reasons. First, the Court found that the material in question is not transmitted “through” Napster, as required by the *DMCA*.⁵⁸ Second, the Court found no evidence that Napster had a policy to address copyright issues, such as blocking users who were known to infringe copyright or

⁴⁸ *Ibid.*

⁴⁹ *Ibid.*

⁵⁰ (7 December 1999), No. C99-5183 NHPADR (Cal. Dist. Ct.).

⁵¹ See “Napster for Windows: Getting Started,” online: Napster <www.napster.com/help/win/gettingstarted> (date accessed: 19 October 2001).

⁵² *Ibid.*

⁵³ For a full description of how Napster works, see the explanation of Chief Justice Patel in *A & M Records, Inc. v. Napster, Inc.*, 114 F. Supp.2d 896 (Cal. Dist. Ct. 2000).

⁵⁴ I.F. Koenigsberg, D.E. Case & S. Mentzer, “Music, the Internet, and the Music Industry” (2000) 640 *Practising Law Institute/PAT* 9 at 18.

⁵⁵ *Supra* note 50. See also *ibid.*

⁵⁶ *Ibid.*

⁵⁷ *Ibid.*

⁵⁸ *Ibid.*

implementing software to distinguish copyright material and to block the transmission of such material.⁵⁹

Napster also relied on the decision in the *Sony* case to argue that its software had significant non-infringing uses and was, therefore, protected by the “fair use” doctrine of American copyright law. The RIAA countered this argument by leading evidence from a study that 87 percent of all Napster users engage in copyright infringement.⁶⁰

The Court found that while Napster was liable for secondary copyright infringement, some of Napster’s functions, such as the search engine and location tool, provide for non-infringing uses, which may qualify for protection under the *DMCA*.

On appeal, the Ninth Circuit of the United States Court of Appeals found that Napster was also liable for direct and contributory copyright infringement and that the copying of protected material was not saved by the “fair use” doctrine or the *DMCA*.⁶¹ In response, the U.S. District Court in California ordered that Napster block files that contain copyright works within three business days of receiving notice that the work is protected by copyright.⁶²

In response to the order, the RIAA sent Napster a list of 135,000 songs to be blocked from its service.⁶³ Napster began blocking these files by employing keyword filters that determine whether the filename contains the title or artist’s name of copyrighted material. While this solution reduced the amount of copyright material available on the Napster service, this method of filtering contains fundamental problems. While Napster can use filters that block access to files containing the names of certain artists or song titles, the filters are unable to block copyright files that have had their filenames altered.

The ease with which someone can frustrate such filters is found in software created by the Canadian company PulseNewMedia.⁶⁴ The software simply alters the filename of MP3 files resident on a user’s computer by moving the last letter of the filename to the front of the filename. Since Napster’s filters only screen for keywords based on an artist’s name or song title, they fail to block filenames that have been modified. Thus Napster users can continue to download copyrighted works. While Napster could update its filters to include such altered filenames, Napster users could simply further modify the filenames by running the program a second time and creating a second generation alteration. It is likely that further modifications to filenames created by loyal Napster users will continue to outpace the filters’ ability to adequately screen for new and evermore innovative alterations to filenames.

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

⁶¹ *A & M Records, Inc. v. Napster, Inc.* 239 F.3d 1004 (9th Cir. App. 2001).

⁶² [2001] WL 227083 (Cal. Dist. Ct.), online: WL (DCT).

⁶³ See “Canada firm uses pig Latin to fool Napster block,” online: CNN.COM/SCI-TECH <www.cnn.com/2001/TECH/internet/03/12/napster.02/index.html> (date accessed: 4 November 2001).

⁶⁴ *Ibid.*

New network technologies have also emerged which frustrate the music industry's attempts to stop copyright infringement on the Internet. Network technologies such as "Gnutella" create decentralized networks, which allow users to connect to each other rather than to a central server.⁶⁵ Accessing the Gnutella network involves connecting directly to another personal computer on the network, which is connected to another computer and so on, in a "daisy-chain fashion."⁶⁶ It is common for each computer to be linked to three computers at a time, creating a web of users, each acting as a server.⁶⁷ When a user searches for a file on the network, the search request is sent along the chain until the file is found, at which time a direct connection is made with the computer that hosts the desired file and the downloading begins.⁶⁸ Unlike Napster, blocking or filtering material on such decentralized networks is virtually impossible since there is no single point in the network where a filter can be applied successfully.⁶⁹ Shutting down the service would necessarily involve blocking each individual from connecting to the network.

A successful solution, therefore, must focus not on the filename of the copyright audio file as Napster has attempted, but on the data contained within the file itself. This would also prevent networks such as Gnutella from circumventing copyright legislation simply by employing a technological architecture that makes legal action impractical.

B. WIPO

In order to meet the demands of new technologies, the World Intellectual Property Organization ("WIPO") adopted the comprehensive *WIPO Copyright Treaty* in December of 1996.⁷⁰ The Treaty will come into force three months after 30 states have formally ratified it.⁷¹ As of January 24, 2002, thirty-one states had ratified the treaty, which will come into force on March 6, 2002.⁷² While Canada is a signatory, it has not yet ratified the treaty. The preamble of the Treaty succinctly captures the rationale behind the need to harmonize international copyright law, stating that there exists "the need to introduce new international rules and clarify the interpretation of certain existing rules in order to provide adequate solutions to the questions raised by new economic, social, cultural and

⁶⁵ See "What is Gnutella?," online: Gnutella <www.gnutella.co.uk/about/> (date accessed: 4 November 2001).

⁶⁶ See "Hungry for Music? A Look at Napster alternatives," online: CNN.COM/SCI-TECH <www.cnn.com/2001/TECH/internet/05/04/napster.alternatives.idg/index.html> (date accessed: 4 November 2001).

⁶⁷ *Ibid.*

⁶⁸ *Ibid.*

⁶⁹ H. Siegel & B. Semel, "He Share, She Share: Sorting out the State of Music File-Swapping Online After Napster" (2001) 18:3 *e-commerce* 1, online: WL (ECOMMERCE).

⁷⁰ *WIPO Copyright Treaty*, 20 December 1996, online: WIPO <www.wipo.org/eng/diplconf/distrib/94dc.htm> (date accessed: 19 October 2001).

⁷¹ *Ibid.*, art. 20.

⁷² *Contracting Parties of Treaties Administered by WIPO*, online: WIPO <www.wipo.int/treaties/docs/english/s-wct.doc> (date accessed: 18 February 2002).

technological developments.”⁷³ The Treaty also recognizes “the need to maintain a balance between the rights of authors and the larger public interest.”⁷⁴

The relevant provision for the purposes of on-line musical works is found in Article 11 of the Treaty. Article 11 of the Treaty declares that states

shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.⁷⁵

C. INTERNATIONAL EFFORTS

The American *Audio Home Recording Act*, discussed above, which implemented a SCMS to prevent multi-generational copying of copyrighted works, is consistent with its obligations under Article 11 of the *WIPO Copyright Treaty*. The United States has also passed the *Digital Millennium Copyright Act*, discussed above, which prohibits the production or sale of devices designed to evade technological measures for limiting reproduction of, and access to copyright works. Canada, however, has yet to pass any such legislation.

In March of 2000, the European Council adopted a Directive paving the way for the ratification of the *WIPO Copyright Treaty*.⁷⁶ The European Council legislation confidently states that the implementation of the WIPO agreement “will help to ensure a balanced level of protection for works and other subject matter, while allowing the public access to material available via networks.”⁷⁷

The Australian government has also passed legislative changes to strengthen its copyright laws to account for new technological advances. Introduced in 1999 and in force as of March 4, 2001,⁷⁸ the *Copyright Amendment (Digital Agenda) Act 2000*⁷⁹ strengthens Australian copyright law by outlawing devices and software that would bypass encryption and other security technology. Australia’s legislative scheme also limits liability for ISPs much like the American *DMCA*.⁸⁰

⁷³ *Supra* note 70, Preamble.

⁷⁴ *Ibid.*

⁷⁵ *Supra* note 70, art. 11.

⁷⁶ EC. Council Decision 00/278 of 16 March 2000 on the approval, on behalf the European Community, The *WIPO Copyright Treaty*, and the *WIPO Performances and Phonograms Treaty*, [2000] O.J. L. 89/6.

⁷⁷ *Ibid.*, s. 1.

⁷⁸ *Information Sheet G65 Digital Agenda amendments: an overview*, online: Australian Copyright Council <www.copyright.org.au/PDF/InfoSheets/G065v02.pdf> (date accessed: 5 April 2001).

⁷⁹ *Copyright Amendment (Digital Agenda) Act 2000* (Aust.), 2000.

⁸⁰ See *supra* note 78.

IV. CANADIAN PROTECTION

As previously mentioned, the music industry in Canada is worth almost \$1 billion per year and, consequently, copyright protection is as important domestically as it is in the United States. Canadian legislation has been slow, however, to adapt to the changes in technology that have occurred recently and may be ill equipped to handle the issues that have arisen in the United States.

A. COPYRIGHT LAW IN CANADA

Copyright is protected in Canada under the *Copyright Act*,⁸¹ first enacted in 1921. It grants specific rights to “every original literary, dramatic, musical and artistic work.”⁸² Copyright law encompasses works in various mediums and includes protection for public performances, sound recordings, and broadcast signals. Copyright laws encourage the creation of original works by granting the author exclusive rights to exploit and thereby profit from his or her original work. A musical work is defined as “any work of music or musical composition, with or without words, and includes any compilation thereof.”⁸³ For most works, copyright extends for 50 years from the end of the calendar year of the death of the author.⁸⁴

While sound recordings have not traditionally been recognized worldwide, the *Copyright Act* has included them. Section 18 of the *Copyright Act* grants copyright to “the maker of a sound recording.”⁸⁵ The *Copyright Act* states that “the maker of a sound recording has a copyright in the sound recording.”⁸⁶ The copyright holder of the sound recording has the sole right to publish it for the first time, reproduce it in any material form, and rent it out.⁸⁷ The *Copyright Act* defines the “maker” of a sound recording as “the person by whom the arrangements necessary for the first fixation of the sounds are undertaken.”⁸⁸ Section 2.11 of the *Copyright Act* defines “arrangements,” as it pertains to makers of sound recordings, as being those financial and technical arrangements necessary for the first fixation of the sounds.⁸⁹

Section 15 of the *Copyright Act* grants copyright to a performer of her performance of the work.⁹⁰ Performance is defined as “any acoustic or visual representation of a work, performer’s performance, sound recording or communication signal, including a representation made by means of any mechanical instrument, radio receiving set or television receiving set.”⁹¹

⁸¹ R.S.C. 1985, c. C-42 [hereinafter *Copyright Act*].

⁸² *Ibid.*, s. 5(1).

⁸³ *Ibid.*, s. 2.

⁸⁴ *Ibid.*, s. 6.

⁸⁵ *Ibid.*, s. 18(1).

⁸⁶ *Ibid.*

⁸⁷ *Ibid.*, ss. 18(1)(a)-(c).

⁸⁸ *Ibid.*, s. 2.

⁸⁹ *Ibid.*, s. 2.11.

⁹⁰ *Ibid.*, s. 15(1).

⁹¹ *Ibid.*, s. 2.

A recorded musical work such as a song, therefore, would engage copyright protection under multiple sections. For example, the lyrics of the song would be protected under the guise of “literary, dramatic or musical work” under s. 3(1) of the *Copyright Act*, which include various rights.⁹² Literary and musical rights include the right to “produce, reproduce, perform or publish any translation of the work,”⁹³ and the right “to communicate the work to the public by telecommunication.”⁹⁴ The sound recording would be protected separately under s. 18 and includes the right to publish it for the first time and to reproduce in the recording in any material form.⁹⁵ The performance of the musical work would also attract protection under s. 15 of the *Copyright Act*, which would protect the performer from unauthorized reproduction.⁹⁶ Ultimately, the unauthorized copying of a song can potentially infringe several copyrights and damage the revenue of various parties.

The *Copyright Act*, however, provides for limited rights to copy material otherwise protected under the law. Section 80 of the *Copyright Act* makes it legal to reproduce a musical work where it is “for the private use of the person who makes the copy.”⁹⁷ Under domestic law, therefore, it is completely acceptable to make a copy of a copyright musical work for personal use, as it is under the “fair use” doctrine of the United States as interpreted in the *Sony* case. Section 29 of the *Copyright Act* also sets out the “fair dealing” exceptions, which, for example, allow for the copying of material for the purpose of research or private study and for the performance of copyright material under certain circumstances.⁹⁸

B. CANADA’S OBLIGATIONS UNDER THE *WIPO COPYRIGHT TREATY*

In response to the signing of the *WIPO Copyright Treaty* in December of 1997, Industry Canada commissioned two Canadian copyright experts to provide their opinion on the amendments needed to the *Copyright Act* if Canada were to ratify the Treaty.⁹⁹ Johanne Daniel and Lesley Ellen Harris discussed Canada’s obligation pertaining to the *WIPO Copyright Treaty*.¹⁰⁰ Their paper concluded that domestic copyright law did not offer protection to copyright works from devices or conduct designed to circumvent copyright protection technology.¹⁰¹ For this reason, the authors reasoned that the *Copyright Act* should be amended to prohibit devices or conduct that would circumvent technological measures (such as encryption or access codes) to prevent unfettered access to copyright works.

⁹² *Ibid.*, ss. 3(1)(d)-(f).

⁹³ *Ibid.*, s. 3(1)(a).

⁹⁴ *Ibid.*, s. 3(1)(f).

⁹⁵ *Ibid.*, ss. 18(1)(a) and (b).

⁹⁶ *Ibid.*, s. 15.

⁹⁷ *Ibid.*, s. 80.

⁹⁸ *Ibid.*, ss. 29, 29.5, i.e., a not-for-profit performance related to an educational institution.

⁹⁹ Industry Canada, *The Implementation of the WIPO Copyright Treaty* (Discussion Paper) by J. Daniel & L.E. Harris (Ottawa: Industry Canada, 1998), online: Industry Canada <strategis.ic.gc.ca/SSG/ip01038e.html> (date accessed: 19 October 2001).

¹⁰⁰ *Ibid.*

¹⁰¹ *Ibid.*

Proposals discussed in the paper included making it “an infringing act to remove or bypass, for infringing purposes, any device or measure intended to limit reproduction, [performance in public or communication to the public]/[or any other right granted under the *Copyright Act*] of a work or other subject matter.”¹⁰² The proposal also included making it an infringing act to transmit a work knowing that technological protections have been bypassed.¹⁰³

A second proposal called for legislating against importing, manufacturing, or distributing a device or providing a service that had the capability of circumventing copyright protection technology where the purpose of the technology was to limit reproduction.¹⁰⁴

These proposals would protect copyright protection technology not only from devices meant to bypass reproduction-limiting technology, but also from conduct where a party knows that technology has been circumvented. While such amendments to the *Copyright Act* would satisfy Canada’s obligations to the *WIPO Copyright Treaty*, they would not go as far as the United States and its implementation of the *Audio Home Recording Act*. These proposals would prohibit devices in Canada and users in Canada from defeating a SCMS, but the proposals would not mandate that devices in Canada incorporate an SCMS. There is a material difference between manufacturing a device that simply does not incorporate an SCMS, and manufacturing a device that will specifically bypass an encryption system on a musical file to prevent copying. In this regard, the proposed changes to the *Copyright Act* fall short of the efforts made in the United States.

In response to the need for legislative change to address these technological issues, the Intellectual Property Policy Directorate of Industry Canada and the Copyright Policy Branch of Canadian Heritage issued a consultation paper on digital copyright issues on June 22, 2001.¹⁰⁵ The paper considered issues regarding regulation of technology and invited responses to its proposals. The paper “considered the possibility of restricting or prohibiting the traffic in circumvention devices, while at the same time permitting devices that have, as their primary purpose, an activity that qualifies as legitimate” and declared that the “difficulty is that devices which are suited to infringing uses are, by and large, equally suited to non-infringing uses.”¹⁰⁶ The paper also stated that Industry Canada and Canadian Heritage question the ability for a copyright framework to adequately restrict devices that permit the illegitimate copying of material, while protecting the legitimate exceptions allowed by the *Copyright Act*.

As will be discussed below, a SCMS would address the concerns of copyright holders and those weary of limiting the exceptions for fair dealing and private use. The incorporation of an SCMS would allow the device to distinguish the making of an

¹⁰² *Ibid.*

¹⁰³ *Ibid.*

¹⁰⁴ *Ibid.*

¹⁰⁵ See Industry Canada and Heritage Canada, *Consultation Paper on Digital Copyright Issues* (Ottawa: Industry Canada, 2001), online: Industry Canada and Heritage Canada <strategis.ic.gc.ca/SSG/rp01099e.html> (date accessed: 4 November 2001).

¹⁰⁶ *Ibid.*, c. 4.2.

authorized copy from an unauthorized use. Mandating that hardware can only make a copy of a musical work from the original work would strike a balance between the privilege allowed under s. 80 of the Canadian *Copyright Act*, while limiting the ability to make multi-generational copies of a work. The incorporation of an SCMS scheme such as the one in the American *AHRA*, therefore, is a logical extension to the Canadian *Copyright Act*. One such SCMS that could be implemented with the co-operation of recording companies and music distributors is discussed below. The government, therefore, should not hesitate to implement such a solution.

V. OTHER SOURCES OF PROTECTION

A. SECURE DIGITAL MUSIC INITIATIVE

While the implementation of the proposals discussed above would inhibit the production of devices capable of bypassing copyright technologies, a viable solution to the copyright infringement created by the supply of MP3s must include co-operation from music distributors.

To this end, a group of recording companies, software and hardware developers, and on-line services have created a forum called the "Secure Digital Music Initiative" ("SDMI") to combat the problem of digital copyright infringement.¹⁰⁷ The purpose of the initiative is to bring "together the worldwide recording, consumer electronics and information technology industries to develop open technology specifications for protected digital music distribution."¹⁰⁸ The SDMI plans to introduce a rights management system consisting of digital watermarking that SDMI compliant hardware will recognize in order to distinguish original sound recordings from pirated copies.¹⁰⁹ The SDMI also aims to set a series of technological rules that will apply to all digital music devices and programs in order to play music files.¹¹⁰ These rules would be variable and could be programmed by the producer of the compact disc or MP3 file. For example, a music group who wanted to promote its music by freely distributing its music could program their MP3s with a code that allows for multiple free copying. Record producers, on the other hand, could encode MP3s with time sensitive instructions so that the file will only be playable for a specified amount of time once downloaded or with instructions that the file can only be played a specific number of times. Embedded instructions could also mandate that the copying of the file would be prohibitive altogether.

Another benefit to the encryption of music files is the ability to track the file electronically.¹¹¹ This end-to-end tracking would allow the owners of the copyright in

¹⁰⁷ W.M. Pollack, "Tuning In: The Future of Copyright Protection for Online Music in the Digital Millennium" (2000) 68 *Fordham L. Rev.* 2445 at 2473.

¹⁰⁸ See "Frequently Asked Questions," online: SDMI <www.sdmi.org/FAQ.htm> (date accessed: 3 December 2000).

¹⁰⁹ *Ibid.*

¹¹⁰ *Ibid.*

¹¹¹ J. Selby, "The Legal and Economic Implications of the Digital Distribution of Music: Part 2" (2000) 11:2 *Ent. L. Rev.* 25 at 27.

the musical work to track the movement of copies after the recording has been sold.¹¹² A royalty management system could then be implemented to accurately distribute financial royalties depending on the number of times a musical work had been copied.¹¹³ While file tracking would be an attractive advantage to music publishers, the privacy concerns regarding the tracking of a user's listening habits would have to be addressed.¹¹⁴

The transition towards the proposed SDMI technology would occur in two stages.¹¹⁵ First, hardware and software capable of playing digital music would be released that would recognize the watermarks and encryption technology proposed by the SDMI, but which would still be able to play unencrypted music files. Once music files containing the new encrypted material became available, a software upgrade would be necessary in order to listen to the new encrypted music files. The software upgrade would subsequently prohibit the playing of illegitimate sound recordings that did not contain a digital watermark. This two-step process would ease the industry into new encryption technology and provide for compatibility until music files with digital watermarks became widely available.

With the co-operation of the recording industry and music producers, most of whom are participants in the initiative, compact discs and on-line music will soon be encoded with SDMI protocols.

The SDMI is an example of how the market will play a role along with government in helping to prohibit the pirating of MP3s. Once SDMI becomes standard protocol, compact discs and on-line music files will contain a digital watermark complete with copyright information. If Canada implements amendments to the *Copyright Act* to ensure adherence to the *WIPO Copyright Treaty*, software and hardware developed domestically and imported into Canada would be prohibited from circumventing this encoded copyright information.

Domestic law could also be strengthened by requiring that hardware and software developed or imported into Canada use the SDMI protocol as its designated SCMS. This would ensure that devices and computer programs capable of playing MP3s would only recognize CDs and MP3s encoded with legitimate copyright information.

Therefore, while it would be possible to make an MP3 backup of a song from a CD, the copy would lack the relevant copyright information. This would make it impossible

¹¹² *Ibid.*

¹¹³ *Ibid.*

¹¹⁴ The issue of privacy on the Internet and privacy in general is beyond of the scope of this article. For a discussion of privacy, see generally S.D. Warren & L.D. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. Rev. 193; C. Fried, "Privacy" (1968) 77 Yale L.J. 475; J. Kang, "Cyberspace Privacy: A Primer and Proposal" (1999) 26 *Human Rights* 3; J. Litman, "Information Privacy/Information Property" (2000) 52 Stan. L. Rev. 1283; J.R. Redenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace" (2000) 52 Stan. L. Rev. 1315; J.D.R. Craig, "Invasion of Privacy and Charter Values: The Common-Law Tort Awakens" (1997) 42 McGill L.J. 355 and P. Burns, "The Law of Privacy: The Canadian Experience" (1976) 54 Can. Bar Rev. 1.

¹¹⁵ Pollack, *supra* note 107 at 2473.

to make a copy from this first-generation copy. Even if the user posted the MP3 onto a personal web page or attempted to transfer the file via Napster, the resultant copy would be unplayable. Similarly, users who attempted to download MP3s from the personal libraries of other users over the Internet would be unable to play the songs as they would lack the digital watermark encoded on the music file needed for the SDMI-based MP3 player to actually play the MP3 file.

While requiring that a SCMS, such as those mandated by the SDMI, be built into new hardware and software would extend Canada's laws beyond its responsibilities under the *WIPO Copyright Treaty*, it would further harmonize domestic laws with those of the United States. Legislating that a SCMS scheme be incorporated into new technologies in the same way as it is mandated by the American *AHRA* would protect the owners of copyright better than simply prohibiting devices and conduct which bypassed such technology. Such a statutory scheme would also nicely complement the legislation needed for Canada to adhere to its *WIPO Copyright Treaty* obligations.

There are concerns, however, that the implementation of legislative changes prohibiting circumvention technology, such as the provisions under the *DMCA*, would inhibit rights under the fair dealing sections of the *Copyright Act*.¹¹⁶ For example, while an educational institution has the right to reproduce a work for the purposes of research under s. 29 of the *Copyright Act*, it would be unable to take advantage of these rights if legislation that prohibited anticircumvention technology was implemented. A user permitted to make a copy under the fair dealing doctrine would thus be deprived of her right.

A solution to this problem, however, can be found in legislation enacted in Australia. As previously discussed, Australia's implementation of the *Copyright Amendment (Digital Agenda) Act 2000* prohibited devices capable of circumvention of technological protection measures. The legislation, however, provides an exception "if the recipient of the device or service makes a written declaration that the device or service is only to be used for a 'permitted purpose,'" and a "permitted purpose" includes certain activities by educational institutions, libraries, governments, and decompilers of software.¹¹⁷ Such an exception strikes a harmonious balance between the needs of copyright holders in limiting access to copyright material with those wanting to utilize their fair dealing rights. Amendments under Canadian law could prohibit circumvention technology, such as provided under the *DMCA*, while allowing for those who have a right under the fair dealing doctrine to take advantage of the legislative exceptions.

B. BLANKET ROYALTY SCHEMES

While the above proposals would reduce the amount of piracy in MP3s, copyright infringement will never cease to exist. To this effect, domestic law could also implement

¹¹⁶ See, e.g., M. Perry & C. Chisick, "Copyright and Anti-circumvention: Growing Pains in a Digital Millennium" (2000) N.Z.I.P.J. 261 as well as the concerns expressed by the Consultation Paper on Digital Copyright Issues, discussed above at *supra* notes 105-106 and accompanying text.

¹¹⁷ *Supra* note 78.

a royalty scheme to compensate artists and recording companies for copyright infringement. A similar scheme exists in s. 82 of the Canadian *Copyright Act*, which imposes a levy on every "blank audio recording medium" sold in Canada.¹¹⁸ Section 79 defines "audio recording medium" as "a recording medium, regardless of its material form, onto which a sound recording may be reproduced and that is of a kind ordinarily used by individual consumers for that purpose, excluding any prescribed kind of recording medium."¹¹⁹ A "blank audio recording medium" is further defined as "an audio recording medium onto which no sounds have ever been fixed" and "any other prescribed audio recording medium."¹²⁰ While the blanket levy takes into account the fact that blank tapes are occasionally used for the copying of copyright material and compensates the relevant parties accordingly, it only applies to blank audio tapes and CDs. It does not take into account the proliferation of new technology devices such as any future "Rio" type player that could serve the same function as blank audio tapes. In this regard, if Canada wishes to adequately compensate parties for copyright infringement, a levy should also be placed on new medium recording devices. A blanket royalty scheme such as the one imposed by the American *AHRA* would serve to mitigate the impact of piracy in MP3s and other forms of new media. Such a royalty could be made to apply only to devices capable of recording digital music, much like the *AHRA*, so as to limit its affect on devices which simply play back music.

VI. ISP LIABILITY

"Internet Service Providers (ISPs) play an integral role in enabling use of the Internet, whether the user is a sender of content or a recipient."¹²¹ ISPs act as intermediaries and provide the network services that enable users to connect to the Internet. ISPs provide a variety of services for their subscribers.¹²² At a minimum, ISPs provide access to the Internet, which allows users to surf the World Wide Web, transmit and receive information, and use various programs to send and receive e-mail.¹²³ Many ISPs also provide their subscribers with space on their servers so that they can create and maintain their own web sites.¹²⁴

There are various reasons why owners of copyright material would choose an action against an ISP rather than the person who actually posted the infringing material. First, unlike Internet users, ISPs are relatively easy to locate. While the structure of the Internet allows a user who downloads copyright material anonymity, the ISP is relatively easy to find. An action against a corporate ISP may also provide for a greater possibility of financial compensation than an action against an individual user. Extending liability to ISPs may also provide incentives to block access to copyright material or to remove copyright material located on its servers.

¹¹⁸ *Supra* note 81, s. 82.

¹¹⁹ *Ibid.*, s. 79.

¹²⁰ *Ibid.*

¹²¹ *Supra* note 105 at c. 4.4.

¹²² *Ibid.*

¹²³ *Ibid.*

¹²⁴ *Ibid.*

There are problems, however, with extending liability to ISPs that act as mere conduits for subscribers to access the Internet. Most of the technical processes involved in the transmission of information are automated and the ISP may be unaware of the copyright material at the time it is transmitted. The sheer amount of material transmitted across the Internet is also prohibitive to the screening of material. Rogers, for instance, allows subscribers 300 megabytes of data transmission per month. Considering the fact that Rogers has almost 350,000 subscribers in Canada, screening every transmission would require a marked increase in resources.¹²⁵

A. INTERNATIONAL EFFORTS ON ISP LIABILITY

On June 8, 2000, the European Union ("EU") adopted Directive 2000/31/EC, which outlined the liability to be imposed on ISPs in different situations.¹²⁶ Article 12 of the Directive provides ISPs with an exemption from liability where they act merely as conduits to the transmission of information. Article 12 states that where an ISP's service "consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network," the ISP will not be liable for the information that is communicated.¹²⁷ To be afforded protection under this clause, however, the ISP must ensure that it does not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission.¹²⁸ The Directive broadens the term "provision of access" 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 provided that the information is not stored for any period longer than is reasonably necessary for the transmission."¹²⁹ This clause ensures that an ISP can operate efficiently by allowing it to perform the necessary technological function of temporarily storing the information on its server as the information is transmitted. This Article does not, however, prevent the denial of service by an ISP to a subscriber who has been found transmitting or receiving infringing material.¹³⁰

The Directive also limits liability to ISPs that offer hosting services to their subscribers. Article 14 of the Directive states that liability shall not be imposed where information is stored by the ISP at the request of a subscriber provided that the ISP does not have actual knowledge of illegal activity or material and that "upon obtaining such knowledge ... acts expeditiously to remove or to disable access to the information."¹³¹ Article 15 of the

¹²⁵ "Rogers upgrades network to boost reliability," online: Communications, Engineering & Technology <www.cedmagazine.com/ced/2001/0701/07c.htm> (date accessed: 4 November 2001).

¹²⁶ EC, *Council Directive 00/31 of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the International Market (Directive on electronic commerce)*, [2000] O.J. L. 178/1.

¹²⁷ *Ibid.*, art. 12.

¹²⁸ *Ibid.*

¹²⁹ *Ibid.*, art. 12(2).

¹³⁰ *Ibid.*, art. 12(3).

¹³¹ *Ibid.*, art. 14(1)(b).

Directive, however, prohibits Member States from requiring ISPs to monitor material hosted on their servers.¹³²

The United States has also enacted legislation attempting to balance the rights of ISPs and users of the Internet. The *DMCA*, discussed above, provides "safe-harbors" for ISPs. Section 512(k)(1)(A) of the *DMCA* limits liability for ISPs that merely act as conduits for users to connect to the Internet.¹³³ The requirements for protection include that the user initiate the transmission, the process be automatic, that the ISP not select the recipient, that no copy is maintained by the ISP, and that the material is not modified in transit.¹³⁴

The *DMCA* also protects ISPs that provide storage services for users on their servers.¹³⁵ Section 512(c) of the *DMCA* protects ISPs from liability where there is no actual knowledge of infringing material, the ISP is unaware of facts that make infringement apparent, and the ISP acts expeditiously upon notice to remove or block access to the infringing material.

These safe harbors apply only if the ISP has adopted and reasonably implemented procedures to terminate the service of repeat infringers.¹³⁶ The safe harbor provisions provide a complete bar to monetary damages and restrict the availability of injunctive relief while maintaining the fair use doctrine. Section 512(c)(3) also provides for detailed notice and take-down procedures to facilitate the requirements under s. 512(c). To discourage unfounded take-down notices, s. 512(c) also ensures that misrepresentations with regards to take-down notices are actionable.

B. CANADIAN EFFORTS ON ISP LIABILITY

Currently, Canadian copyright legislation is limited in its treatment of liability that may be imposed on ISPs. Section 2.4(1)(b) of the *Copyright Act* states that "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 that work or other subject matter to the public."¹³⁷

¹³² *Ibid.*, art. 15.

¹³³ *DMCA*, *supra* note 32, § 512(k)(1)(A). This section defines an ISP for the purposes of this safe harbor as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."

¹³⁴ *Ibid.*

¹³⁵ For the purpose of this safe harbor, the *DMCA* § 512(k)(1)(B) defines the service provider as "a provider of online services or network access, or the operator of facilities therefor." The broader definition is a result of the fact that the ISP is providing additional services vis-à-vis the services provided by an ISP, than acts as a mere conduit and thus cannot be captured within the more narrow definition of § 512(k)(1)(A), which deals with ISPs that act as mere conduits of communication.

¹³⁶ *Ibid.*, § 512(i).

¹³⁷ *Supra* note 81, s. 2.4(1)(b).

The Canadian Copyright Board addressed the issue of ISP liability under section 2.4(1)(b) of the *Copyright Act* in the *Tariff 22, Internet* decision of October 1999.¹³⁸ The case dealt with the communication of musical works over the Internet and who should pay the tariff associated with the communication. The Board considered the exception provided to ISPs under section 2.4(1)(b) of the *Copyright Act* and how broadly to define the term “means of telecommunication.”¹³⁹ Proponents of *Tariff 22* argued that section 2.4(1)(b) applied “only to the provision of physical facilities used by others to communicate a work to the public” and did not include the actual service provided by ISPs.¹⁴⁰ Under this narrow interpretation, commercial ISPs would not qualify for the limitation of liability under the *Copyright Act* as their services consist of more than simply providing the physical means of communication. Alternatively, opponents of *Tariff 22* contended that anyone who operated the facilities or physical equipment, or provided the services necessary to facilitate the transmission, was not involved in the communication of the material and was thus protected from liability by the *Copyright Act*.¹⁴¹

The Copyright Board agreed with the opponents of *Tariff 22* that the “means” referred to under s. 2.4(1)(b) were not limited to merely physical facilities. “They include all software connection equipment, connectivity services, hosting and other facilities and services without which such communications would not occur.”¹⁴² The Copyright Board, therefore, found that an ISP is not precluded from relying on the exemption simply because it provides ancillary services or performs steps such as caching to improve performance.¹⁴³ “As long as its role in respect of any given transmission is limited to providing the means necessary to allow data initiated by other persons to be transmitted over the Internet, and as long as the ancillary services it provides fall short of involving the act of communicating the work or authorizing its communication, it should be allowed to claim the exemption.”¹⁴⁴

While the *Tariff 22* decision may partially address the issue of ISP liability in Canada, there are significant problems with relying solely on this decision to address ISP liability. First, the decision can be appealed to, and subsequently overturned by, the Federal Court of Canada. To this effect, the Federal Court of Canada is currently deliberating an appeal of this decision of the Copyright Board. Second, the exception in the *Copyright Act*, and subsequently any decision based on that section, dealt solely with ISP liability where the ISP acts merely as a conduit for the transmission. The *Copyright Act* and the *Tariff 22* decision are silent with regards to the liability that will be imposed on ISPs where they provide web site hosting services and are found to be hosting infringing material on their servers. Unlike the EU Directive and the American *DMCA*, which address the requirements of actual knowledge and notice and take-down provisions, Canadian ISPs

¹³⁸ *Re SOCAN Statement of Royalties, Public Performance of Musical Works 1996, 1997, 1998 (Re Tariff 22, Internet)* 1 C.P.R. 4th 417 [hereinafter *Tariff 22*].

¹³⁹ *Ibid.* at 443.

¹⁴⁰ *Ibid.* at 451.

¹⁴¹ *Ibid.*

¹⁴² *Ibid.* at 452.

¹⁴³ *Ibid.*

¹⁴⁴ *Ibid.*

do not have the comfort of legislative guidance as to their obligations with respect to these issues under Canadian law.

Additionally, amending copyright laws in Canada without addressing these issues would further place ISPs in a precarious position. If Canada implements an amendment to the *Copyright Act* that prohibits the dissemination of hardware or software that is designed to circumvent encryption technology, ISPs could potentially be held liable for a breach of this legislative scheme. For example, if an Internet user posted a piece of illegal software onto his web page, hosted by his ISP, the ISP could potentially be held liable for housing the illegal program on its server and making it available to the public. In order to protect ISPs from such liability where they have no knowledge of the infringing activity, Canada must ensure that limited ISP protection is enacted as part of a potential statutory scheme, much like provisions in the *DMCA* in the United States. Holding ISPs responsible for material present on their servers and available through web pages they host would burden ISPs with the task of policing their servers for pirated material. This would add expense to providing Internet service, which could subsequently be passed onto the end user, limiting Internet access for many individuals.¹⁴⁵ “Inflicting strict liability standards on OSPs [Online Service Providers] where they act as passive carriers and can not, through reasonable effort, be aware of the nature of the content transmitted via their systems, would substantially affect their cost of providing services and may drive many out of business.”¹⁴⁶

The government of Canada must address the serious issue of ISP liability with legislative change. Legislation should consider the obligations of ISPs in different situations and provide a framework for notice and take-down procedures. The legislative changes must also consider the liability of ISPs where procedures have not been followed and the liability on users who make misrepresentations on notices to ISPs of infringements. These are issues that cannot be adequately addressed by simply interpreting current provisions of the *Copyright Act*. Relevant legislation must strike an adequate balance between limiting liability on ISPs, while requiring that they have procedures in place to remove infringing material once they become aware of such material.

VII. CONCLUSION

The Internet has ushered in a technological revolution, which has made the dissemination of information effortless. The costs of providing and obtaining information have decreased dramatically as the costs of accessing new technology has dropped substantially. The expansion in the size of the average hard drive as well as the development of sound compression technology has made it economically viable to store large personal libraries of music files. The speed of average Internet access has also increased dramatically, thanks to developments in broadband technology. Software programs and network technologies such as Napster and Gnutella have made finding and copying MP3s quick and easy while threatening to undo the entire domestic copyright

¹⁴⁵ M. Jakobson, “Copyright Liability of Online Service Providers After the Adoption of the E.C. Electronic Commerce Directive: A Comparison to U.S. Law” (2000) 11:7 Ent. L. Rev. 144 at 146.

¹⁴⁶ *Ibid.*

regime with regards to music files. A solution, however, is viable. The technological advances of the Secure Digital Music Initiative will soon make encrypted copyright information standard on every compact disc available for sale. By prohibiting the production of hardware or software with the capabilities to bypass the copyright information, while legislating that software and hardware available domestically incorporate an SCMS such as the SDMI protocols, the piracy of digital music will be greatly reduced. Canada must incorporate these proposals as well as limit ISP liability and offer blanket royalties to ensure that an adequate balance is maintained in protecting the interests of all the relevant parties. By incorporating legislation that addresses the issues of the *WIPO Copyright Treaty*, and by adopting schemes that have been implemented internationally, Canada will help ensure that this balance is maintained.