PART THREE

Creativity

CHAPTER TWELVE

"Modernizing" ISP Copyright Liability

Gregory R. Hagen*

A. INTRODUCTION

In the intense battle for the spoils generated by the online information ecosystem, it has been a contentious question as to whether Internet intermediaries — especially those who carry, host and index others' information — should be liable for copyright infringement in relation to content provided by third parties. Internet intermediaries include Internet access providers, web hosting providers, Internet payment systems, search engines, portals, e-commerce intermediaries, blogs, video sites, and social networking platforms.[1] Currently, under the *Copyright Act*,[2] those who provide the means necessary for others to communicate works and other subject matter on the Internet (Internet Service Providers or ISPs) will not be liable for copyright infringement if they *merely* provide such means.[3] Under the *Copyright Act*, there are no mandatory notice and takedown (NTD) provisions requiring ISPs to prevent infringement by taking down

* I gratefully acknowledge the financial support of Borden Ladner Gervais, the research assistance of Kimberly Howe, and the helpful comments from an anonymous reviewer, Michael Geist, Sam Witherspoon and Maria Lavelle.

1 More generally, Internet intermediaries bring together or facilitate transactions between third parties on the Internet. *See* Organization for Economic Co-Operation and Development, "The Economic and Social Role of Internet Intermediaries" (April 2010), www.oecd.org/dataoecd/49/4/44949023.pdf.

2 *Copyright Act*, R.S.C. 1985, c. C-42, http://laws.justice.gc.ca/en/C-42 [*Copyright Act*].

3 *Ibid.*, ss. 2.4(1)(b).

allegedly infringing subject matter when an allegation is received from a copyright owner. Nor is there a notice and notice (NN) system which requires ISPs to forward a notice from a copyright owner of alleged infringement by its customer, in relation to the use of the ISP's facilities, to the allegedly infringing customer. Nonetheless, it has been common practice for a number of years for major ISPs to voluntarily forward a notice of alleged infringement to their customers.[4]

Bill C-32, the *Copyright Modernization Act*,[5] clarifies the liability of Internet intermediaries by adding new immunity provisions for ISPs and search engines. "ISPs and search engines are exempt from liability when they act strictly as intermediaries in communication, caching and hosting activities."[6] By implication, the immunity under Bill C-32 will apply to access providers, hosts, bloggers, video sites, social networking sites and others who communicate third party content and merely act as ISPs. Search engines are treated differently and can enjoy immunity from liability for damages, but are subject to injunctions.[7] Further, the Bill introduces a new form of secondary liability for Internet Intermediaries who know or ought to know that their services are designed primarily to enable copyright infringement.[8] The possibility that ISPs might be found liable for infringement as *authorizers* of infringing activity by others remains.

Further, the Government of Canada comments that "ISPs are in a unique position to facilitate the enforcement of copyright on the Internet."[9] In particular, they are the only parties that can identify and notify subscribers accused of infringing copyright by using the ISPs services.[10] Bill C-32, therefore, mandates a NN system under which an ISP (excepting search engines) must, without delay, forward notices of alleged infringement to

---

4 Bell, Rogers, Shaw and Telus, "Submission of Bell, Rogers, Shaw and Telus," www.ic.gc.ca/eic/site/008.nsf/eng/02634.html ["Submission of Bell, Rogers, Shaw and Telus"].

5 Bill C-32, *Copyright Modernization Act*, 3d Sess., 40th Parl., 2010, www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4580265&file=4 [Bill C-32].

6 Canada, Balanced Copyright, "Copyright Modernization Act — Backgrounder" (June 2010), http://www.ic.gc.ca/eic/site/crp-prda.nsf/eng/h_rp01151.html ["Copyright Modernization Act — Backgrounder"].

7 Bill C-32, above note 5, s. 47. Note, however, the limitations to this partial immunity discussed later in this paper.

8 Bill C-32, above note 5, s. 18. (See proposed s. 27(2.3)).

9 Canada, Balanced Copyright, "What the New Copyright Modernization Act Means for Internet Service Providers, Search Engines and Broadcasters" (June 2010), http://www.ic.gc.ca/eic/site/crp-prda.nsf/eng/rp01188.html ["Balanced Copyright"].

10 *Ibid*.

the customers they concern,[11] but ISPs will not be required to take down allegedly infringing content. Nor will ISPs be required to limit or terminate access when they are notified of allegedly infringing conduct of their subscribers under a graduated response system (GR). ISPs will also be required to preserve evidence of the identity of alleged infringers for a period of up to six months, or one year if the content creator commences an action.[12] If an ISP fails to follow the notice procedures, it risks being held liable for an award of damages.[13]

Most striking is the fact that the new secondary liability provision will be ineffective against highly decentralized, peer to peer file sharing networks, such as those using the bitTorrent protocol, because there is no central, coordinating entity that can be found liable. Instead, the primary means of enforcing copyright against peer to peer file sharing networks under the Bill is to control the information itself rather than its distribution through ISPs. This approach, which is suggested by the World Intellectual Property Organization (WIPO) Internet Treaties, builds upon the ability of copyright owners to use technological measures or "digital locks" to control access to their works and other subject matter.[14] Since infringers can also use tools to circumvent such measures, the Bill prohibits the circumvention of digital locks that control access to works and other subject matter.[15] Given a generative Internet,[16] though, one in which individuals are able to quickly respond and adapt to digital locks, it will be a challenge, if indeed it is possible, for private interests to succeed in controlling access to information while serving copyright's goals and maintaining privacy, free expression, fair procedures and the rule of law. That is a topic for a different paper, however.

---

11 Bill C-32, above note 5, s. 47. (See proposed s. 41.26.)

12 *Ibid*. (See proposed s. 41.26(1)(b).)

13 *Ibid*. (See proposed s. 41.26(3).)

14 *WIPO Copyright Treaty*, 20 December 1996, www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html, 36 I.L.M. 65 at Art. 8; *WIPO Performances and Phonograms Treaty*, 20 December 1996, www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html, 36 I.L.M. 76, Art. 16(2).

15 Bill C-32, above note 5, s. 47. (See proposed s. 41.1(1).)

16 "Generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences." See Jonathan Zittrain, "The Generative Internet" (2006) 119 Harv. L. Rev. 1974–2040, www.harvardlawreview.org/issues/119/may06/zittrain.shtml at 1980.

B. BACKGROUND

The Internet is an engine of dissemination of information that can benefit the public. As the Supreme Court of Canada said in the *SOCAN* decision, "The capacity of the Internet to disseminate "works of the arts and intellect" is one of the great innovations of the information age. Its use should be facilitated rather than discouraged."[17] However, as the world transitions to a global, digitally-networked information economy, the winners from the old economy are striving to ensure that the benefits from the new economy will accrue to them.[18] Rather than focus on the Internet as a remarkable disseminator of information, many copyright owners are concerned that the Internet has displaced their traditional dominance as distributors of content, diminishing their ability to maximize their revenues.

Copyright owners, therefore, emphasize the Supreme Court's important proviso to its statement above that the dissemination of works "should not be done unfairly at the expense of those who created the works of arts and intellect in the first place."[19] Associations, such as the International Chamber of Commerce, urge that "[i]ntellectual property (IP) theft is a huge and growing global challenge."[20] Canada in particular has been singled out by the International Chamber of Commerce as a "major source of the world's piracy problem."[21] The United States 2010 Special 301 Watch List refers to "the continuing challenges of Internet piracy in countries such as Canada."[22] Canada's copyright laws are often (unjustly) touted to be weak[23] and its failure to ratify the 1996 WIPO Internet Treaties is often

17 *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, http://csc.lexum.umontreal.ca/en/2004/2004scc45/2004scc45.html, [2004] 2 S.C.R. 427 at para. 40 [*SOCAN* cited to S.C.R.].

18 See Yochai Benkler, "The Battle Over the Institutional Ecosystem in the Digital Environment" (2001) 44 Communications of the ACM 84–90, www.benkler.org/CACM.pdf.

19 *SOCAN*, above note 17 at para. 40.

20 International Chamber of Commerce, "International Chamber of Commerce Urges G8/G20 Action on Counterfeiting and Piracy" (22 June 2010), http://smr.newswire.ca/en/international-chamber-of-commerce-and-canadian-intellectual/international-chamber-of-commerce-urges-g8g20-action.

21 International Federation of the Phonographic Industry, "IFPI reacts to publication of draft Canadian Copyright Amendment Bill," (June 2010), www.ifpi.org/content/section_news/20100607.html. For a useful counterpoint, see Michael Geist, "Piracy Haven Label Case of Rhetoric Over Reality" (10 May 2010), www.michaelgeist.ca/content/view/5020/159.

22 United States, United States Trade Representative, *2010 Special 301 Report* (April 2010) at 1, www.ustr.gov/webfm_send/1906.

23 Barry Sookman, "Copyright Reform for Canada: What Should We Do?" www.ic.gc.ca/eic/site/008.nsf/eng/02934.html [Sookman, "What Should We Do?"]. For a useful

criticized.[24] Some politicians have even argued (wrongly) that ratifying the WIPO Internet Treaties is required by international law.[25]

Given the Internet, the ability of copyright owners to maintain control of the distribution of their copyrighted subject matter depends upon their control of Internet communications. However, the ability to control the communication and reproduction of works and other subject matter via the Internet is limited because, unlike conventional telecommunications systems, the Internet was designed without a central point of control.[26] Early Internet theorists believed that the distributed architecture of the Internet rendered it impossible to regulate.[27] Others emphasized that the Internet's architecture — its code — could be changed, making it regulable.[28] Still others countered that Internet intermediaries were natural points of control that could be used to regulate their customers and potentially could be found liable for acts of copyright infringement.[29]

Copyright owners have used various arguments to justify regaining control over the communication of information over the Internet. Access to information, including copyrighted content, on the Internet is a powerful inducement for people to sign up with an access provider,[30] an inducement from which ISPs profit. Copyright owners have claimed that ISPs authorize infringing activity and, therefore, should be considered liable

---

rebuttal, see Howard Knopf, "The Annual 301 Show — USTR Call for Comments — 21 Reasons Why Canadian Copyright Law is Already Stronger than USAs" (February 2010), http://excesscopyright.blogspot.com/2010/02/annual-301-parade-ustr-calls-for.html.

24 *Ibid*.

25 See Gregory R. Hagen, "A Note on Integrity in Treaty-Making & Copyright Law" (11 March, 2008), http://ablawg.ca/2008/03/11/a-note-on-integrity-in-treaty-making-copyright-law/#more-81.

26 Keenan Mayo & Peter Newcomb, "How the Web Was Won" *Vanity Fair* (July 2008), www.vanityfair.com/culture/features/2008/07/internet200807.

27 David R. Johnson & David G. Post, "Law and Borders — The Rise of Law in Cyberspace" (1996) 48 Stan. L. Rev. 1367–1402, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=535. See also John Perry Barlow, "A Cyberspace Declaration" (February 1996), http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

28 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

29 Jack Goldsmith & Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

30 *SOCAN*, above note 17 at para. 121.

for infringement.[31] More practically, copyright owners argue that access providers are an "efficient engine of collection"[32] of copyright royalties.

The well-known judgment of the Supreme Court of Canada in *SOCAN* suggests that the copyright liability of ISPs who carry, host and cache third party content should be based primarily upon principles of fault. First, since ISPs, as common carriers, merely carry the communications of others, they do not themselves communicate copyrighted subject matter. Second, ISPs are innocent disseminators of information in defamation law, similar to bookstores, libraries, and news vendors who have no actual knowledge of defamation and have not been negligent in failing to detect the defamation.[33] According to the Supreme Court in *SOCAN*: "To the extent they act as innocent disseminators, they are protected."[34] A well-known common law principle applied to copyright would hold that, as between two innocent parties, the copyright owners and ISPs, losses should normally lie where they fall, with the copyright owners.[35] Third, it is impractical, both economically and technically, to monitor the deluge of information transmitted through an intermediary.[36] Finally, immunity from infringement encourages intermediaries to "expand and improve their operations without the threat of copyright infringement."[37] Consequently, disputes between copyright owners and consumers should not be "visited on the heads of the Internet intermediaries" (i.e., ISPs).[38]

In response, copyright owners and their lobbyists have pressed their case for creating a new form of copyright liability against ISPs who facilitate infringement, especially peer to peer file sharing services.[39] One lobbyist for the Canadian Recording Industry Association, has suggested that "secondary infringement doctrines are essential for pursuing pirate

---

31 *Ibid.*

32 *Ibid.* at para. 3.

33 *Ibid.* at para. 95.

34 *Ibid.* at para. 95.

35 Oliver Wendell Holmes, *The Common Law* (Chicago: ABA Publishing, 2009), www.gutenberg.org/etext/2449 at 34.

36 *SOCAN*, above note 17 at para. 101.

37 *Ibid.* at. para. 114.

38 *Ibid.* at para. 131.

39 The US position is that the *Anti-Counterfeiting Trade Agreement* "is not intended to include new intellectual property rights or to enlarge or diminish existing intellectual property rights." See the Office of the US Trade Representative, "Statement of ACTA Negotiating Partners on Recent ACTA Negotiations" (1 July 2010), www.ustr.gov/about-us/press-office/press-releases/2010/june/office-us-trade-representative-releases-statement-act.

online sites and services."[40] At the same time, copyright owners and their lobbyists have also called for a stronger role for ISPs who are merely information conduits in policing infringement by others over their networks. Some lobbyists continue to insist that a formalized NTD regime, in addition to a NN regime, would benefit copyright users.[41] They have also advocated for a series of graduated responses to alleged copyright infringement that could result in limiting or cutting off Internet access.[42]

C. THE *COPYRIGHT MODERNIZATION ACT*

1) General

How does the *Copyright Modernization Act* modernize the role of ISPs? In introducing the *Copyright Modernization Act,* the Government of Canada billed it as a "key pillar" in the Canadian Government's strategy to make Canada a leader in the "global digital economy."[43] In *Improving Canada's Digital Advantage*, copyright is described as "an important marketplace framework law and cultural policy instrument that must give Canadian creators, citizens, and consumers the tools they need to compete in the global digital economy."[44] According to such a market-based approach, copyright creates a private property right as a reward for the investment of intellectual labour.[45] It is "individuals' right to protect their own creations."[46] The role of ISPs in the digital economy is to "disseminate cre-

---

40 See Sookman, "What Should We Do?" above note 23. While there are no explicit provisions in the *Copyright Act* concerning liability for inducing infringement or materially contributing to copyright infringement, Sookman comments that "[i]t is probable, but uncertain, that Canadian law provides relief for acts that induce or materially contribute to copyright infringement." This is not the case as, under s. 89 of the *Copyright Act*, copyright is limited to the rights provided for under the *Copyright Act* and remedies are provided only for violation of those rights.

41 *Ibid.*

42 Barry Sookman & Dan Glover, "Graduated response and copyright: an idea that is right for the times," *The Lawyers' Weekly* (January 2010), www.barrysookman.com/2010/01/20/graduated-response-and-copyright-an-idea-that-is-right-for-the-times [Sookman and Glover, "Graduated Response and Copyright"].

43 Canada, Balanced Copyright, "Government of Canada Introduces Proposals to Modernize the Copyright Act" (June 2010), www.ic.gc.ca/eic/site/crp-prda.nsf/eng/h_rp01149.html [*Balanced Copyright*].

44 Canada, Digital Economy Consultation, *Improving Canada's Digital Advantage,* http://de-en.gc.ca/wp-content/uploads/2010/05/Consultation_Paper.pdf at 28, emphasis added [*Improving Canada's Digital Advantage*].

45 *Ibid.* at 28.

46 P2Pnet, "James Moore vs. Radical Extremists," www.p2pnet.net/story/41150.

ative content and connect people across Canada and the world."[47] In short, copyright creates products for a digital market and ISPs are the means by which those products are licensed by copyright owners.

At the same time that ISPs enable the marketing of digital products they can enable copyright infringement by others. A "well-functioning marketplace," on the Government's view, would secure copyright owners against the "stealing" of their products.[48] At its extreme, this view entails that all social benefits of a copyright should accrue to its owner. It implies that, even if inexpensive dissemination of art, literature, music, software and films greatly benefitted individuals in society but cost copyright owners a little (or at least failed to benefit them), the dissemination would be unjustified. The implication of such a view for ISP liability, as Nesbitt pointed out years ago, is that "[a]ny statutory limitation on the liability of ISPs would, according to this [natural rights] perspective, represent a degradation of the protected rights of a copyright owner. . . ."[49] Although the Government of Canada may not push its market-based view to its extreme,[50] its aim is that Canadian companies be able to compete in a global digital market in copyrighted products wherein copyright owners largely control the product and its dissemination.

This world view is, in reality, rather antiquated. The idea that copyright is a common law property right that results from the application of intellectual labour was popular in the second half of the eighteenth century but was rejected by the House of Lords in *Donaldsen v. Becket*.[51] More recently the view that copyright is concerned *only* with the prevention of free riding off the intellectual labour of authors was rejected by the Supreme

47 *Balanced Copyright,* above note 43.

48 *Improving Canada's Digital Advantage,* above note 44 at 14.

49 Scott Nesbitt, "Rescuing the Balance? An Assessment of Canada's Proposal to Limit ISP Liability for Online Copyright Infringement" (2003) 2 Canadian Journal of Law and Technology 115 at 124, http://cjlt.dal.ca/vol2_no2/pdfarticles/nesbitt.pdf.

50 For instance, under the proposed s. 29 of the Bill, there are several new fair uses for education, parody and satire, non-commercial user-generated content, format shifting, time shift and backup copies.

51 *Donaldson v. Beckett*, 2 Brown's Parl. Cases 129, 1 Eng. Rep. 837; 4 Burr. 2408, 98 Eng. Rep. 257 (1774), www.copyrighthistory.com/donaldson.html.

Court of Canada[52] and by prominent copyright scholars.[53] Finally, the idea that reproduction and communication technologies, such as ISPs, need to be controlled to prevent the dissemination of certain kinds of works is as old as the Stationer's Company and its censorship of heretical books.[54] Ironically, the *modern* idea that copyrighted content should be freely available in return for compensation to owners provided by a levy or from a compulsory license fee is given short shrift.[55]

The Government's view of the role of copyright in a digital economy might explain its desire for liability for peer to peer file sharing services, but it does not explain its particular choice of a secondary liability provision. The Minister of Heritage says that "[t]he best way to fight piracy is by targeting those who knowingly enable online infringement."[56] Why is that? Why did it not include seemingly stronger secondary infringement provisions such as liability for contributory infringement[57] and for induce-

---

52 *Théberge v. Galerie d'Art du Petit Champlain inc.*, 2002 SCC 34, http://csc.lexum.umontreal.ca/en/2002/2002scc34/2002scc34.html, [2002] 2 S.C.R. 336 at para. 30 [*Théberge* cited to S.C.R.]. The Supreme Court remarked at para. 31 that Canada copyright law is a balance between "promoting the public interest in the encouragement and dissemination of works of art and the intellect" and "obtaining a just reward for the creator."

53 Mark Lemley, "Property, Intellectual Property and Free Riding" (2005) 83 Tex. L. Rev. 1031, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=582602. As Lemley has suggested, to obtain the full social value of works and other subject matter is as fair as charging all pedestrians for viewing the roses in one's garden.

54 Lionel Bently and Brad Sherman, *The Making of Modern Intellectual Property Law: The British Experience, 1760–1911* (Cambridge: Cambridge University Press, 1999) at 11–12.

55 The role of free information on the internet has been discussed at length by Lawrence Lessig, *The Future of Ideas: the Fate of the Commons in a Connected World* (Toronto: Random House, 2001). A right to remuneration for music file sharing was proposed by the Songwriters Association of Canada in "Our Proposal: Detailed" (29 March 2009) http://songwriters.ca/proposaldetailed.aspx. See also the specific proposals by Neil Netanel, "Impose a Noncommercial Use Levy to Allow Free Peer-to Peer File Sharing," (2003) 17:1 Harvard Journal of Law & Technology 1, http://jolt.law.harvard.edu/articles/pdf/v17/17HarvJLTech001.pdf; and William W. Fisher III, *Promises to Keep: Technology, Law, and the Future of Entertainment* (Stanford: Stanford University Press, 2004).

56 James Moore, "Minister Moore's Speech at Luncheon on Intellectual Property, Innovation, Economic Growth, and Jobs Toronto, Ontario June 22, 2010," www.pch.gc.ca/pc-ch/minstr/moore/disc-spch/index-eng.cfm?action=doc&DocIDCd=SJM100603 ["Moore's Speech"].

57 Liability for contributory infringement exists where a third party with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another. See *Gershwin Publishing Corp. v Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

ment to infringe[58] as in the US? If it is merely because that is not a Commonwealth country approach, why not adopt the Australian approach to authorization, one that is more favourable to copyright owners? Perhaps the Government wanted to find only the clearly faulty liable — those whose know or ought to know that their service is designed primarily to enable infringement. But, then the question that remains is whether ISPs can be liable for authorizing the infringing activity of others by failing to prevent that activity (e.g. by taking down files that are hosted) when given notice of it? Why did the Bill not include a NTD system or GR system for ISPs? Perhaps the Government of Canada believes that the forms of secondary liability are practically equivalent and sufficient to effectively diminish online infringement. Perhaps it heeded the criticisms of NTD and GR systems. More likely, though, is that in its vision of the digital marketplace, it is satisfied that copyright owners will be able to control the digital products themselves using digital locks even if not able to control totally the distribution of their products through third parties.

2) TSP Immunity under the *Copyright Act*

a) TSPs Don't Infringe

The *Copyright Modernization Act* supplements, but does not replace, an existing immunity provision in the *Copyright Act*. In order to better understand the new immunity provision, it is useful to briefly describe the existing provision. The *Copyright Act* currently does not explicitly grant an immunity to ISPs but, rather, to those persons "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."[59] These intermediaries might be termed "Telecommunications Service Providers" or "TSPs." Section 2.4(1)(b) of the *Copyright Act* deems that TSPs do not communicate:[60]

> 2.4 (1) For the purposes of communication to the public by telecommunication,

58 Inducement liability exists when one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps to foster infringement, is liable for the users' resulting acts of infringement. See *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Inc.* 545 U.S. 913, www.supremecourtus.gov/opinions/04pdf/04-480.pdf, (2005) 125 S.Ct. 2764 [*Grokster*].

59 *Copyright Act*, above note 2, s. 2.4(1)(b) (emphasis added).

60 *Ibid.*

> . . .
>
> (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 that work or other subject-matter to the public; . . . .

Section 2.4(1)(b) was originally intended to protect TSPs who acted as intermediaries between broadcasters and retransmitters of broadcast signals.[61] One of the main issues in *SOCAN* was whether TSPs included ISPs (who act in a content neutral way). In *Electric Despatch*, the Supreme Court of Canada ruled that the owners of telephone wires cannot be said to transmit a message the meaning of which they were ignorant.[62] Counsel to SOCAN argued before the Federal Court of Appeal, however, that section 2.4(1)(b) of the *Copyright Act* was intended merely to protect traditional common carriers, such as poles, cables and wires, from liability for the content of the communications that they transmitted rather than to the newer Internet intermediaries, such as Rogers, Shaw, Telus and Bell.[63] In *SOCAN*, the Supreme Court of Canada held broadly that "the *Copyright Act* . . . does not impose liability for infringement on intermediaries who supply software and hardware to facilitate use of the Internet."[64] Or, to put it differently, it ruled — in essence — that neutral ISPs are TSPs. In particular, the Court said: [65]

> So long as an Internet intermediary does not itself engage in acts that relate to the content of the communication, i.e., whose participation is content neutral, but confines itself to providing "a conduit" for information communicated by others, then it will fall within s. 2.4(1)(b).

---

61 Canada. House of Commons, Sub-Committee on the Revision of Copyright of the Standing Committee on Communications and Culture, *A Charter of Rights for Creators* (Ottawa: House of Commons, 1985) at 80, cited in *SOCAN*, above note 17 at para. 90.

62 *Electric Despatch Co. of Toronto v. Bell Telephone Co. of Canada* 1891 CanLII 11, (1891), 20 S.C.R. 83 at 91, www.canlii.org/en/ca/scc/doc/1891/1891canlii11/1891canlii11.html.

63 *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2002 FCA 166, [2002] 4 F.C. 3 at para. 120, www.canlii.org/en/ca/fca/doc/2002/2002fca166/2002fca166.html.

64 *SOCAN*, above note 17 at para. 101.

65 *Ibid.* at para. 92.

The court also held that section 2.4(1)(b) of the *Copyright Act* applies to caching and hosting by ISPs since they are reasonably useful and proper to achieve the benefits of enhanced economy and efficiency, [66] provided that these activities are content neutral.[67]

It is worth emphasizing that the Supreme Court declined to characterize section 2.4(1)(b) of the *Copyright Act* as an immunity from liability for what would otherwise be an infringing *act*.[68] If section 2.4(1)(b) applies, an ISP does not communicate; rather the person who posts a file communicates it.[69] Similarly, the Federal Court of Appeal recently held that "[i]n providing access to "broadcasting," ISPs do not transmit programs."[70] The Federal Court of Appeal referred to section 4(4) of the *Broadcasting Act*, a common carrier provision analogous to section 2.4(1)(b) in support of its view.[71] However, the Court also made the more general point that the finding that content-neutral transmission intermediaries do not transmit in *Electric Despatch* itself implies that ISPs are not broadcasters.[72] The Federal Court of Appeal ruling suggests that whether an ISP reproduces, communicates, broadcasts, distributes or otherwise acts is a matter of fact, not of law. An ISP can be found liable for copyright infringement when it is more than a mere conduit.[73] As the Supreme Court of Canada noted, section 2.4(1)(b) of the Act protects the function of an ISP, not ISPs *per se*.[74] Similarly, an ISP could be found to be broadcasting if its role was no longer content neutral.[75]

b) Limited Exception: Authorization

Under section 27(1) of the *Copyright Act*, it is an infringement of copyright for anyone to do anything that is the sole right of a copyright owner, including

66 *Ibid.* at paras. 104–19.
67 *Ibid.* at para. 92.
68 *Ibid.*, at para. 87.
69 *Ibid.* at para. 111.
70 *Canadian Radio-television and Telecommunications Commission (Re),* 2010 FCA 178 at para. 59, www.canlii.org/en/ca/fca/doc/2010/2010fca178/2010fca178.html.
71 *Ibid.* at para. 44. A "telecommunications common carrier" is in turn, defined in subsection 2(1) of the *Telecommunications Act* as "a person who owns or operates a transmission facility used by that person or another person to provide telecommunications services to the public for compensation."
72 *Ibid.* at para. 47.
73 *SOCAN*, above note 17 at para. 92.
74 *Ibid.*, at para. 102.
75 *Ibid.* at para. 59.

authorizing the exercise of an owner's rights.[76] Consequently, ISPs may be found liable if they authorize infringing acts of their subscribers. In *SOCAN*, the Supreme Court of Canada dealt with the question of whether ISPs authorize the downloading of musical works and sound recordings by merely providing the infrastructure necessary for communicating them.[77] In order to answer the question, the Court analogized the situation to another that was discussed in an earlier decision, *CCH*, in which the issue was whether the Law Society of Upper Canada library authorized patrons to make a copy of a work by providing a photocopier.[78] It ruled that authorization requires that one "sanction, approve and countenance" the infringing activity.[79] But what kind of acts of an Internet intermediary constitute authorization?

First, the Court decided in *CCH* that a person does not authorize infringement by merely authorizing the use of equipment that *could* be used to infringe copyright. A similar result was reached earlier by the UK House of Lords when it found that a seller of dual cassette recorders did not authorize reproductions of cassettes since the seller had "no control over the use of their models once they are sold."[80] Applying the reasoning from *CCH* in the Internet context, the Supreme Court found in *SOCAN* that when a massive amount of non-copyrighted material is available to the end user, one cannot impute an authorization to download copyrighted material solely based upon the provision of "Internet facilities." [81] This reasoning applies not only to internet access providers but to other ISPs who communicate content from third parties, including the *Globe and Mail*, YouTube, Google, Facebook, Amazon, eBay and others.

Second, the additional fact that someone who provides a service has *knowledge* that someone *might be using* its service to infringe copyright is not sufficient to constitute authorization by the intermediary. Presumably, in *CCH*, the library could have instituted a system whereby a librarian acts as a gatekeeper to prevent infringement, but it did not and no authorization was found.[82] Later, in *SOCAN,* the Supreme Court stated that "[t]he knowledge that someone might be using neutral technology to violate

---

76 *Copyright Act*, above note 2, s. 27(1).

77 *SOCAN*, above note 17 at para. 121.

78 *CCH Canadian Ltd. v. Law Society of Upper Canada,* 2004 SCC 13, http://csc.lexum.umontreal.ca/en/2004/2004scc13/2004scc13.html , [2004] 1 S.C.R. 339 at para. 38 [*CCH* cited to S.C.R.].

79 *Ibid.* at para. 38.

80 *CBS Songs Ltd v Amstrad Consumer Electronics plc*, [1988] 2 All ER 484 (H.L.), at 492–94.

81 *SOCAN*, above note 17 at para. 123.

82 *CCH*, above note 78.

copyright (as with the photocopier in the *CCH* case) is not necessarily sufficient to constitute authorization. . . ."[83] In coming to this conclusion, the Supreme Court explicitly rejected the reasoning of the Australian High Court in *Moorhouse*[84] which had ruled that where a university library knew or had reason to suspect that the photocopiers it provided were likely to be used for purposes of committing an infringement and could have prevented infringement, but failed to do so, the university infringed.[85]

It follows that, under Canadian law, an internet file sharing service that knew that someone *might* be using its services to infringe copyright and could have prevented the infringement by *adding* a component to filter out copyrighted works, but did not, does not thereby authorize infringement. This contrasts, notably, with the *Sharman* decision of the Australian Federal Court of Appeal in which Sharman, which licensed KaZaA file sharing software to end users, was found liable for authorizing infringement by its users where it knew that its users might be infringing copyright, could have prevented it by programming the software to filter out infringing works, but did not do so.[86] In that case, Sharman had no *actual* control over its users' ability to copy particular films, but had *potential* control because it could have programmed its software to filter out particular content from being downloaded.[87]

Third, to conclude from the fact that an ISP who has knowledge that its service *might* be used to infringe copyright, an ability to prevent infringement by others using the service, and a failure to prevent such infringement, that the ISP infringes is unsound because that service could be used for legal purposes. Even if the supply of an Internet service *did* authorize sharing of copyrighted materials, "[c]ourts should presume that a person who authorizes an activity does so only so far as it is in accordance with

---

83 *SOCAN*, above note 17 at para. 127.

84 *Moorhouse v. University of New South Wales*, [1976] R.P.C. 151.

85 *CCH*, above note 78 at para. 41.

86 *Universal Music Australia Pty Ltd. v. Sharman License Holdings Ltd.* (with Corrigendum dated 22 September 2005), [2005] FCA 1242 (5 September 2005) [*Sharman*]. The *Copyright Act 1968* (Australia), section 101(A), requires that in determining whether a person has authorized infringement, the following must be considered: (a) the extent (if any) of the person's power to prevent the doing of the act concerned; (b) the nature of any relationship existing between the person and the person who did the act concerned; (c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.

87 *Ibid* at para. 414.

the law."[88] Such legal purposes include downloading public domain or licensed works or downloading for the purposes of fair dealing and for uses that fall under the private copying provision of the *Copyright Act*.[89]

Fourth, according to the Supreme Court, in *CCH*, "[t]his presumption may be rebutted if it is shown that a certain relationship or degree of control existed between the alleged authorizer and the persons who committed the copyright infringement."[90] Of central import, of course, are the sources and the degree of control necessary for rebuttal. Elsewhere in the judgment, the Court points to additional sources of possible control: control over which works a user may copy and control over the purposes of copying.[91] It follows that, when an ISP has specific knowledge that it hosts infringing content and the ability to take it down, failure to take it down *might* result in infringement. The Supreme Court stated that "notice of infringing content, and a failure to respond by "taking it down" may in some circumstances lead to a finding of "authorization."" [92] The Court elsewhere said more bluntly that "[i]f the host server provider does not comply with the notice, it may be held to have authorized communication of the copyright material."[93] From the context, a finding of infringement requires actual control over the actions of infringers, rather than merely potential control as in *Sharman*.[94] When the requirements of specific knowledge of infringement and actual control over the acts of infringers are present, there exists a *de facto* NTD system.[95]

---

88 *CCH*, above note 78 at para. 38.

89 For example, one could download the dot torrent file for Canada's Next Great Prime Minister at www.cbc.ca/nextprimeminister/blog/2008/03/download_canadas_next_great_pr.html.

90 *CCH,* above note 78 at para. 38.

91 *Ibid.* at para. 45.

92 *SOCAN*, above note 17 at para. 127.

93 *Ibid.* at para. 110.

94 *Sharman*, above note 86.

95 "Sookman, What Should We Do?" above note 23, and the Entertainment Software Association of Canada, both construe the existing system as a *de facto* NTD system. See Entertainment Software Association of Canada, "Submission to the 2009 Canadian Copyright Consultation by the Entertainment Software Association of Canada," (13 September 2009), www.ic.gc.ca/eic/site/008.nsf/eng/02705.html#p8.3, ["Entertainment Software Submission,"]. By contrast, Sheryl Hamilton considers Canada's system to be one where ISPs are totally immune. See Sheryl N. Hamilton, "Made in Canada: A Unique Approach to Internet Service Provider Liability and Copyright Infringement" in Michael Geist ed., *In the Public Interest* (Irwin Law: Toronto, 2005) 285, www.irwinlaw.com/pages/content-commons/made-in-canada-

A general principle that, given that an ISP has particular knowledge of infringement by its customers in using its services and control over its customers' actions, the failure of the ISP to take action to prevent infringement implies authorization has important limitations. First of all, it may conflict with the legal obligations of ISPs to their customers to provide access and hosting services.[96] Second, a practice of sending unfounded, often automated, notices would undermine the effectiveness of such notices as reliable indicators of infringement.[97] Third, combined with a large number of notices received by Canadian ISPs, it is difficult for ISPs to determine which notices are valid.[98] ISPs would be left only with the knowledge that there might be an infringing use of its services. Left with poor evidence of infringement, ISPs would not have the requisite knowledge of infringement to justify taking down content and risk a breach of contract or, at least, damage to its relationship with its customer. However, the risk remains that if a court judges a notice of alleged infringement to be a reliable indicator of infringement, then failure to take down the content could result in a finding of infringement. ISPs should not be left in this uncomfortable legal limbo.

Finally, it is difficult to define the kind and degree of control that would be necessary to constitute authorization in the context of peer to peer file sharing. Sharman was found liable for authorizing infringement in part because it failed to implement filtering technology in its software.[99] But even under the Australian approach, in some cases it would be too difficult for Internet access providers to control which content is made available through their services to their subscribers. In *iiNet*, for instance, the Australian Federal Court of Appeal held that iiNet, an Internet access provider who knew that its users might infringe copyright by using bitTorrent file sharing clients, did *not* thereby provide the means to infringe.[100] By pro-

-a-unique-approach-to-Internet-service-provider-liability-and-copyright-infringement---sheryl-n-hamilton.

96 *SOCAN*, above note 17 at para. 127.

97 Jennifer M. Urban & Laura Quilter, "Efficient Process or "Chilling Effects"? Take down Notices Under Section 512 of the *Digital Millennium Copyright Act*" (22 December 2008) at 15, http://static.chillingeffects.org/Urban-Quilter-512-summary.pdf.

98 "Submission of Bell, Rogers, Shaw and Telus," above note 4.

99 *Sharman,* above note 86 at para. 414.

100 In *Roadshow Films Pty Ltd v iiNet Limited (No. 3)*, 2010 FCA 24 [*iiNet*], the Australian Federal Court of Appeal held that iiNet, who provided access to the Internet, did not thereby provide the means to copy the works in issue. For discussion, see Julian Gyngell, "Hollywood, the hungry Chinaman, and the ISP" (2010) 5 Journal of Intellectual Property Law & Practice 302.

viding access, it said, iiNet merely provided a *precondition* to the means, which was a bitTorrent file sharing network.[101] In Canada, it would be unlikely that an ISP would be liable for merely providing access to a bitTorrent network for the additional reason that it does not have sufficient degree of control over the content that is carried over its network.

3) Internet Service Provider Immunity "Modernized"

a) The Nature and Scope of Immunity

Section 35 of the Bill introduces an additional immunity for ISPs that is formulated as follows:[102]

> 31.1(1) A person who, in providing services related to the operation of the Internet or another digital network, provides any means for the telecommunication or the reproduction of a work or other subject-matter through the Internet or that other network does not, solely by reason of providing those means, infringe copyright in that work or other subject-matter.

The immunity is not conditioned on the ISP satisfying a NN, NTD or GR regime. The immunity applies more broadly than to just ISPs, as it applies to a service provider utilizing any digital network. Presumably this includes private networks that are not part of the Internet as well as overlay networks on the Internet, including virtual private networks and peer to peer file sharing networks.[103] Finally, it applies to anyone who supplies "any means" for telecommunication rather than to someone who supplies "the means" necessary for telecommunication under section 2.4(1)(b).[104]

The immunity applies to all acts — including reproduction, communication and distribution — that could result in infringement. It is best interpreted as providing an explicitly broader common carrier exemption than does section 2.4(1)(b) of the *Copyright Act*.[105] In other words, on such an interpretation, the provision does not provide an exception from finding that an act infringes, rather, it deems that neutral ISPs *do not engage in any act* above and beyond supplying a means of communication — and so do not infringe copyright.

---

101 *Ibid.* at para 414.

102 Bill C-32, above note 5, s. 35. (See proposed s. 31.1(1).)

103 For simplicity, the remaining discussion will refer to "ISPs" though the context may indicate that it applies to any network service provider.

104 *Copyright Act*, above note 2, s. 2.4(1)(b).

105 *Ibid.*

ISPs are also immune for acts that are *incidental* to providing access. Consequently, the proposed section 31.1(3) provides a similar immunity for an ISP who caches the work or other subject-matter, or who does any similar act in relation to it, to make the telecommunication more efficient does not, by virtue of that act alone, infringe copyright in the work or other subject-matter.[106] The caching immunity is conditioned on caching being a neutral activity.[107] Section 31.1(5) provides immunity for hosts — ISPs do not infringe copyright merely by virtue of hosting.[108] However, this immunity will not apply when a host knows of a decision of a court of competent jurisdiction that the content provider infringes copyright by posting the subject matter or by the way in which the content provider uses that content.[109]

Although Bill C-32 has separate immunity clauses for ISPs and their ancillary services, caching and hosting, in *SOCAN*, the Supreme Court interpreted "the means" of telecommunication referred to in section 2.4(1)(b) of the Act to include "all software connection equipment, connectivity services, hosting and other facilities and services."[110] Caching was also considered to be a necessary means under section 2.4(1)(b) because it is a means that is content neutral and necessary to maximize the economy and cost effectiveness of the Internet conduit.[111] By implication, the new immunity for ISPs should, by implication, apply to their ancillary services.

The Bill contains a distinct form of immunity for Internet search engine providers. Bill C-32 calls search engines "information location tools" and defines them as "any tool that makes it possible to locate information that is available through the Internet or another digital network."[112] Unlike other ISPs, search engines enjoy only a partial immunity contained in section 41.27(1):[113]

> In any proceedings for infringement of copyright, the owner of the copyright in a work or other subject-matter is not entitled to any remedy other than an injunction against a provider of an information

106 Bill C-32, above note 5, s. 35. (See proposed s. 31.1(3).)

107 *Ibid.* (See proposed s. 31.1(4).) Under proposed s. 31.1(4), the immunity does not apply in respect of the work or other subject matter if the ISP modifies it, except for technical reasons; does not comply with executable, automated caching instructions made by the person who made the work or other subject matter available; or interferes with the lawful use of technology to obtain data on its use.

108 *Ibid.* (See proposed s. 31.1(5).)

109 *Ibid.* (See proposed s. 31.1(6).)

110 *SOCAN*, above note 17 at para. 92.

111 *Ibid.*, at para. 115.

112 Bill C-32, above note 5, s. 47. (See proposed s. 41.27(5).)

113 *Ibid.* (See proposed s. 41.27(1).)

> location tool that is found to have infringed copyright by making a reproduction of the work or other subject-matter or by communicating that reproduction to the public by telecommunication.

This immunity differs substantially from the others as it, *prima facie*, merely disentitles the copyright owner from an award of damages. This provision will be discussed in greater detail later.

b) Exception for Services that are Designed Primarily to Enable Infringement

The Bill provides an exception to the immunity that ISPs enjoy. According to the Canadian Government, "[t]he proposed legislation will ensure that those who enable infringement will not benefit from the liability limitations afforded to ISPs and search engines."[114] This is implemented as follows in the *Copyright Modernization Act*:[115]

> 31.1(2) Subsection (1) does not apply in respect of a service provided by the person if the provision of that service constitutes an infringement of copyright under subsection 27(2.3).

Section 27(2.3) creates a new form of secondary liability for services that are primarily designed to enable copyright infringement. This provision will be described and discussed more fully below. A similar exception applies to the immunity for search engine providers.[116]

c) No Exception for Distributing Circumvention Tools

Bill C-32 prohibits the distribution of tools that are used to circumvent technological protection measures or "digital locks."[117] Digital locks control the access to works and other subject matter and restrict the exercise of copyrights and rights of remuneration under the *Copyright Act*.[118] ISPs have complained that section 2.4(1)(b) of the Act, the common carrier exemption, contains no explicit ISP exemption for the distribution of circumvention tools.[119] The proposed common carrier principle, section 31.1(1) of the Bill, does not explicitly exempt ISP from liability for the *distribution* of circumvention tools either.[120] While it is arguable that such a broad common

---

114 "Copyright Modernization Act — Backgrounder," above note 6.
115 Bill C-32, above note 5, s. 35. (See proposed ss. 31.1(2).)
116 *Ibid.* s. 47. (See proposed s. 41.27(4).)
117 *Ibid.* s. 47. (See proposed s. 41.1.)
118 Bill C-32, above note 5, s. 47. (See proposed s. 41).
119 "Submission of Bell, Rogers, Shaw and Telus," above note 4.
120 Bill C-32, above note 5, s. 35. (See proposed s. 31.1(1).)

carrier principle implies that an ISP neither communicates nor *distributes* circumvention tools, it would be preferable if it were made explicit.

4) Secondary Infringement

a) Services Primarily Designed to Infringe

Section 35 of the Bill amends the *Copyright Act* by providing that the immunity under proposed section 31.1(1) of the Bill does *not* apply when someone infringes under proposed section 27(2.3).[121] Section 27(2.3) introduces a new form of secondary liability as follows:[122]

> It is an infringement of copyright for a person to provide, by means of the Internet or another digital network, a service that the person knows or should have known is designed primarily to enable acts of copyright infringement if an actual infringement of copyright occurs by means of the Internet or another digital network as a result of the use of that service.

This is a new form of secondary infringement by enablement where the (secondary) infringement of one party is based upon the primary (or "actual") infringement by another party. Infringement by enablement is not necessarily co-extensive with infringement by authorizing another to infringe. It may be possible to infringe by providing a service which has been designed primarily to infringe without authorizing anyone to engage in infringing acts.[123]

Second, section 27(2.3) of the Bill does not apply to "offline" tools such as personal video recorders, digital cameras, photocopiers, but only to network services.[124] This distinguishes it from US third party infringement doctrines, such as contributory infringement or inducement to infringe, which can occur whether it is online or offline infringement.[125]

Third, this new form of secondary liability is intended to apply to *services* that enable infringement rather than *products*. In other words, while

---

121 Bill C-32, above note 5, s. 35. (See proposed s. 31.1(2).)

122 Bill C-32, above note 5, s. 18. (See proposed s. 27(2.3).)

123 For example, it may be possible to provide a search engine that is designed primarily to enable infringement by locating dot torrent files that, arguably, enables one to download bitTorrent movie files. At the same time, the service may fall short of authorizing others to infringe because the service cannot control which works its users search for or download. See Gregory R. Hagen, "Are bitTorrent Search Engines Liable for Copyright Infringement?" Intellectual Property Review (forthcoming).

124 Bill C-32, above note 5, s. 18. (See proposed s. 27(2.3).)

125 Above, notes 57 & 58.

the provision would catch peer to peer services similar to Grokster, it would not apply to the software which runs on such services. This distinction inherits the wisdom of the US peer to peer filing decisions which have resulted in liability for secondary infringement for some who provide services that facilitate infringement by means of the Internet or another digital network but not for those who provide products which have substantially non-infringing uses.[126]

Fourth, section 27(2.3) operates as an exception to the immunity from liability that ISPs enjoy under section 31.1(1) of the Bill.[127] Unfortunately, Bill C-32 is not explicit that caching and hosting are no longer immune from liability when they are part of a service that is designed primarily to enable infringing conduct. This could lead to the inference that hosts are immune from liability even if they are part of such an enabling system. However, "any means" under the new section 31.1(1) would include hosting and caching.[128] Consequently, the exception to immunity under section 31.1(2) could arguably also apply to caching under section 31.1(3) and hosting under section 31.1(5).[129] This issue needs to be clarified in the Bill.

Finally, although stopping infringement over peer to peer file sharing networks is the object of the provision, [130] it cannot succeed against highly distributed file sharing services, such as those operating in accordance with the bitTorrent protocol.[131] If Napster or Grokster were designed primarily to infringe copyright, the provision may have succeeded against them because they utilized a centralized servers to index content or dis-

---

126 Jonathan Zittrain, "A History of Online Gatekeeping" (2006) 19:2 Harvard Journal of Law and Technology 253, http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

127 Bill C-32, above note 5, s. 35. (See proposed s. 31.1(2).)

128 *Ibid*. s. 35. (See proposed s. 31.1(1).)

129 *Ibid*. (See proposed ss. 31.1(2), 31.1(3), and 31.1(5).)

130 See James Moore, "Moore's Speech," above note 56 describes the object as fighting "piracy." Barry Sookman, in "Some thoughts on Bill-C-32: An Act to Modernize Canada's copyright laws," www.barrysookman.com/2010/06/03/some-thoughts-on-bill-c-32-an-act-to-modernize-canada%E2%80%99s-copyright-laws, describes the Bill as "intended to target pirate services such as illegal peer-to-peer file sharing sites." Michael Geist, "Digital Economy Strategy Consultation Submission" www.michaelgeist.ca/content/view/5193/125 , characterizes the new form of secondary liability as "new liability for BitTorrent search services" at 11.

131 For an introduction to the bitTorrent protocol, see "A Beginners Guide to bitTorrent" www.bittorrent.com/btusers/guides/beginners-guide. For additional difficulties of enforcing copyright against highly distributed file sharing networks, see Gregory R. Hagen and Nyall Engfield, "Canadian Copyright Reform: P2P Sharing, Making Available and the Three-Step Test," (2006) 3:2 UOLTJ 477.

tribute software. Yet, while bitTorrent users may create their individual overlay networks with the intent of enabling infringement by others, and be individually liable for secondary infringement, there is no necessity for a centralized server operator that can be targeted in a bitTorrent network. While some specialized search engines, such as isoHunt, might be caught by this provision, it will not apply to generalized search engines, such as Google, which also can search and find dot torrent files, enabling one to download bitTorrent content files, such as movie files. Nor will it apply to dot torrent search engines which have been designed primarily to find any bitTorrent file, not just Hollywood movie files.[132]

b) Liability Factors

This new form of infringement requires proof that a service is "designed primarily to enable acts of copyright infringement." In other words, the section requires proof that the designer intended the service to primarily enable infringement. Bill C-32 specifies non-exhaustive factors which a court may consider in determining whether a person has infringed copyright under section 27(2.3):[133]

> 27(2.4) In determining whether a person has infringed copyright under subsection (2.3), the court may consider
>
> (a) whether the person expressly or implicitly marketed or promoted the service as one that could be used to enable acts of copyright infringement;
>
> (b) whether the person had knowledge that the service was used to enable a significant number of acts of copyright infringement;
>
> (c) whether the service has significant uses other than to enable acts of copyright infringement;
>
> (d) the person's ability, as part of providing the service, to limit acts of copyright infringement, and any action taken by the person to do so;
>
> (e) any benefits the person received as a result of enabling the acts of copyright infringement; and
>
> (f) the economic viability of the provision of the service if it were not used to enable acts of copyright infringement.

---

132 For a discussion of secondary infringement in the context of peer to peer file sharing see Bob Clark, "Illegal Downloads: Sharing Out Online Liability: Sharing Files, Sharing Risks" (2007) 2 Journal of Intellectual Property Law & Practice 402.

133 Bill C-32, above note 5, s. 18. (See proposed s. 27(2.4).)

These factors appear to be culled from various foreign decisions regarding forms of secondary liability, some of which are distinct from those currently existing under the *Copyright Act* or proposed under the Bill.[134] For example, the factor cited in section 27(2.4)(a) is reminiscent of the test for liability for inducement to infringe established under *Grokster*.[135] As another example, the factor cited in section 27(2.4)(d) is similar to a provision in section 101(A) of the Australian *Copyright Act* according to which "the extent (if any) of the person's power to prevent the doing of the act concerned"[136] must be considered, notwithstanding that the Australian interpretation of authorization was rejected by the Supreme Court of Canada in *SOCAN*.[137] In this respect, the approach of Bill C-32 reflects a trend existing outside of Canada for courts to apply a common set of factors to determine whether a third party is sufficiently connected to an infringing act to be deemed culpable, regardless of the particular form of secondary liability (e.g., inducement to infringe, contributory infringement or authorization).[138] Since secondary infringement by enablement is distinct from extant forms of secondary liability, some of the factors may not be very relevant to showing that a service was designed primarily to enable infringement. Courts will, therefore, need to exercise great care in applying these factors in determining whether a person knows or ought to know that their service is designed primarily to infringe. Specific evidence of intent through, for example, documentary evidence would be of much greater relevance than the application of these factors.

5) Service Provider Regulation: Notice and What?

a) Notice and Take Down and Its Problems

In Canada, there is no legislated, extra-judicial NTD regime requiring that those who host content take it down when provided with a notice alleging copyright infringement. Nor does Bill C-32 propose a NTD system. Any obligation to take down content would arise solely from a remedy imposed by a court to take down such materials. Therefore, a take down notice in

134 For a survey of relevant cases, see Allen D. Nixon, "Liability of Users and Third Parties for Copyright Infringements on the Internet: Overview of International Developments" in Alain Strowell, ed., *Peer to Peer File Sharing & Secondary Liability in Copyright Law* (Cheltenham, UK: Edward Elgar, 2009) at 12–42.

135 *Grokster,* above note 58.

136 *Copyright Act* (Australia) 1986, section 101(A).

137 *CCH*, above note 78 at para. 41.

138 See Nixon, above, note 134 at 37.

Canada generally takes, and will continue to take, the form of a lawyer's demand to take down alleged infringing material, the failure of which could result in the commencement of a copyright infringement suit. [139]

It is worth pointing out that, even though there is no legislated NTD system in Canada, failure to take down content once an allegation has been made can trigger infringement by the ISP in some circumstances. As the Supreme Court of Canada said in *SOCAN,* "notice of infringing content, and a failure to respond by 'taking it down' may in some circumstances lead to a finding of 'authorization.'"[140] Whether ISPs have the *obligation* to take down content is tricky, however, as taking down content may conflict with contractual obligations to customers.[141] As a result, the Court suggested in *obiter dicta,* that enacting a legislated NTD procedure similar to that of the United States and the European Community may be a more effective remedy than litigating the issue of authorization. [142] Many in the copyright industry are in favour of a NTD system on the basis that it is effective and fairer than the existing (arguably) *de facto* NTD system[143] and that it is the only expeditious means of removing or disabling access to infringing content hosted on the Internet.[144]

One major limitation of a NTD system, however, is that it is primarily suited to a server-client architecture where the client posts content to the intermediary's server. It is not effective for dealing with highly distributed peer to peer systems, such as those using the bitTorrent protocol, in which content is *not* hosted by a central server, but by multiple individual computers distributed across the Internet. [145] Even the centralized dot torrent search engines can be eliminated by using bitTorrent clients, such as Tribler, [146] that provide their own keyword searching or by simply using a generalized search engine, such as Google. A similar point can be made regarding "cloud computing" architecture. Under this architecture, an ISP

---

139 For an interesting example of a Canadian demand letter, see "Affidavit of Gary Fung. No. 1" http://isohunt.com/img/legal/Affidavit%20of%20Gary%20Fung%20No.1.pdf at 35–55.

140 *SOCAN*, above note 17, at para. 127.

141 *Ibid.* at para. 127.

142 *Ibid.* at para. 127.

143 "Entertainment Software Submission" above note 95 and Sookman, "What Should We Do?" above note 23.

144 International Intellectual Property Alliance, "2010 Special 301 Report" www.iipa.com/2010_SPEC301_TOC.htm

145 BitTorrent, Inc., "FAQ — BitTorrent Concepts" (2010), www.bittorrent.com/btusers/help/faq/bittorrent-concepts#4n5.

146 See "What is Tribler?" www.tribler.org/trac/wiki/whatIsTribler .

may be legally the host, but may not have any knowledge or control over the physical location of data that is hosted.[147]

The most serious issue that has been pointed out, however, is that the NTD system can be abused. For one thing, it has been used to chill legitimate free expression, including fair dealing and fair use, as well as resulted in disproportionate remedies. [148] A study of the NTD system in the US found that the process provides "a simple and expedient process available to victims and abusers alike, encouraging complainants to shoehorn a variety of ill-fitting claims into copyright."[149] Once a notice is sent, the fear of potential liability can result in the taking down of content solely to minimize the risk of liability rather than on its merits. According to Wendy Seltzer, in the US "the copyright notice-and-takedown regime operates in the shadow of the law, doing through private intermediaries what government could not to silence speech."[150] In the US, these notices are being sent not only to prevent infringement, but to create leverage in a competitive marketplace, to protect rights not given by copyright, such as trade-mark infringement, unfair competition or privacy intrusion, and to stifle criticism, commentary and fair use.[151] There is little reason to think the Canadian experience would be significantly different under a NTD system.[152]

b) The Rejection of Graduated Response

Bill C-32 rejects a GR system, but the Government of Canada does not say why. The impetus for a GR system came when, in 2008, the Recording Industry Association of American said that it would stop suing individuals who infringe on the internet and, since then, has requested that ISPs institute a GR system to respond to allegations of infringement. [153] Such a

---

147 Eric Knorr & Galen Gruman, "What cloud computing really means" *InfoWorld*, www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031.

148 For a discussion of disproportionality, see Hamilton, above note 95.

149 Jennifer M. Urban & Laura Quilter, above note 97 at 15.

150 Wendy Seltzer, "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment" forthcoming, (2010) 23:2 Harvard Journal of Law and Technology, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1577785.

151 *Ibid.* at 14–15.

152 Barry Sookman, "What Should We Do?" above note 23, has argued in favour of a Canadian NTD and that abuse can be minimized by sending notices under penalty of perjury and that one must consider in good faith defences to infringement prior to sending the notice.

153 Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits" *Wall Street Journal* (19 December 2008), http://online.wsj.com/article/SB122966038836021137.html.

system would mandate that ISPs enforce a series of gradually escalating responses to alleged copyright infringement that could include educational notices, bandwidth capping, connection speed capping, protocol blocking, website blocking, and the termination of access.[154] Copyright lobbyists have touted the GR system as an effective and proportionate response to online infringement.[155] Versions of a GR system have been legislated in Taiwan, South Korea, France, New Zealand and the UK, though not all are in force to date.[156] However, the GR approach has been rejected by Hong Kong, Germany, Spain, Sweden as well as the European Parliament.[157]

Graduated response furthers an idea that is implicit in NTD systems: once an ISP is faced with specific knowledge of infringement and the actual power to prevent it, it has a duty to prevent further related infringements. Although graduated response systems may vary from country to country, according to Barry Sookman, the key characteristics of a graduated response system are:[158]

> (1) rights holders monitor P2P networks for illegal downloading activities; (2) rights holders provide ISPs with convincing proof of infringements being committed by an individual at a given IP address; (3) educational notices are sent through an ISP to the account holder informing him or her of the infringements and of the consequences of continued infringement and informing the user that content can be lawfully acquired online; and (4) if the account holder repeatedly ignores the notices, a tribunal may take deterrent action, with the most severe sanctions reserved for a court.

Despite the advantages to copyright owners,[159] several drawbacks have been pointed out. Most importantly, the GR system may interfere with the right to access the internet, which is a central means to exercise one's right

---

154 Sookman and Glover, "Graduated Response and Copyright," above note 42.

155 *Ibid.* According to Sookman, "In the United Kingdom, a test of the graduated response system showed that 70% of customers stopped infringing in the six month period after receiving the first notice, with a further 16% stopping after the second notice."

156 Johnny Ryan and Caitriona Heinl, "Internet access controls: Three Strikes 'graduated response' initiatives," http://cambridge.academia.edu/JohnnyRyan/Papers.

157 Peter K. Yu, "Graduated Response" forthcoming, (2010) 62 Florida Law Review at 3–4, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1579782 [Yu, "Graduated Response].

158 Sookman and Glover, "Graduated Response and Copyright," above note 42.

159 For discussion, see Yu, "Graduated Response," above note 157 and Sookman and Glover, "Graduated Response and Copyright," *ibid*.

to free expression.[160] Second, like an NTD system, to the extent that GR measures are applied extra-judicially, a GR system may be subject to similar abuses that have occurred in the NTD system.[161] On the other hand, if the complaints are subject to review by an administrative panel, there is a risk that the panels could be systemically biased, as occurred with the ICANN Uniform Dispute Resolution Policy.[162] Third, such a system would substantially raise the costs of policing and data retention that ISPs must undertake.[163] Fourth, a GR system could require ISPs to monitor user behaviour which could necessitate the use of deep packet inspection that is privacy invasive.[164] Fifth, a GR system serves to reinforce existing business methods of copyright owners rather than new methods of dissemination, such as compulsory licenses for peer to peer file sharing.[165] Finally, a GR can be disproportionate in its response, cutting off access to essential services provided by the Internet, such as e-mail, banking and VOIP.[166]

c) ISP Notice and Notice

i) The Existing Voluntary NN System

In 2000, the Canadian Association of Internet Service Providers, the Canadian Cable Television Association and the Canadian Recording Industry Association agreed to implement a voluntary notice and notice regime to handle online copyright infringement claims.[167] The success of the NN system is indicated by the fact that copyright owners have rarely, if ever, gone to the next step and enforced their statutory rights in Canadian courts against file sharers.[168] Moreover, in a recent study, seventy percent of file sharers report they would stop if they received a warning note from their

---

160 Yu, "Graduated Response," above note 157 at 15–17.

161 William Patry, *Moral Panics and the Copyright Wars* (Oxford: Oxford University Press, 2009) at 14.

162 See Michael Geist, "Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP," http://aix1.uottawa.ca/~geist/geistudrp.pdf.

163 Yu, "Graduated Response," above note 157 at 13-15.

164 Office of the Privacy Commissioner of Canada. "Review of the Internet traffic management practices of Internet service providers," (18 February 2009) http://dpi.priv.gc.ca/index.php/essays/review-of-the-internet-traffic-management-practices-of-internet-service-providers/.

165 Patry, above note 161 at 12 and Yu, "Graduated Response," above note 157 at 18.

166 Yu, "Graduated Response," above note 157 at 18.

167 Canadian Cable Television Association, "Comments on the Consultation Paper on Digital Copyright Issues" (14 September 2001), http://strategis.ic.gc.ca/eic/site/crp-prda.nsf/fra/rp00336.html.

168 "Submission of Bell, Rogers, Shaw and Telus," above note 4.

ISP.[169] However, since the NN is voluntary, there is a risk that it is not universally followed.

ii) Bill C-32

Bill C-32 rejects both a NTD system and a GR system in favour of a NN system. According to the proposed section 41.25(1), an owner of the copyright in a work or other subject-matter may send a notice alleging infringement to the person who provides the means of telecommunication or is the host.[170] A notice of claimed infringement must be in writing and must identify the individual; identify the allegedly infringing subject matter; state the claimant's interest or right with respect to the copyright in the work or other subject matter; specify the electronic location of the subject matter; specify the infringement that is claimed; specify the date and time of the claimed infringement; and provide any other information that may be prescribed by regulation.[171]

Once received, the recipient would be required to send on the notice to the alleged infringer, if possible. The proposed requirement reads:[172]

> 41.26 (1) A person described in paragraph 41.25(1)(a) [person who provides the means of telecommunication] or (b) [the person who provides the digital memory] who receives a notice of claimed infringement that complies with section 41.25(2) shall, on being paid any fee that the person has lawfully charged for doing so,
>
> (a) without delay forward the notice electronically to the person that the electronic location identified by the location data specified in the notice belongs to and inform the claimant of its forwarding or, if applicable, of the reason why it was not possible to forward it;. . . .

There is no requirement under Bill C-32 to disclose subscriber information upon receiving a notice of alleged infringement as that would be to privacy intrusive.[173] The subscriber is given a chance to remedy the alleged

---

169 *Ibid.*

170 Bill C-32, above note 5, s. 47. (See proposed s. 41.25(1).)

171 *Ibid.* (See proposed s. 41.25(2).)

172 *Ibid.* (See proposed s. 41.26 (1).)

173 In *Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318 (S.C.J.), the court said at para. 11 that "some degree of privacy or confidentiality with respect to the identity of the Internet protocol address of the originator of a message has significant safety value and is in keeping with what should be perceived as being good public policy."

infringement. If that does not happen, the copyright owner is free to commence an action in court.

In *BMG*, the issue of whether a defendant ISP must disclose subscriber names of those who used particular IP addresses is raised. [174] The court adopted the *Norwich Pharmacal*[175] approach to interpreting its own rules of civil procedure authorizing pre-action discovery.[176] On that approach, a person who gets mixed up in wrongdoing, even innocently, is obliged to assist the injured part by providing vital information such as the identity of other persons.[177] The Court held that while privacy concerns must be considered, "they must yield to public concerns for the protection of intellectual property rights."[178] However, in court proceedings, subscriber information can only be disclosed to the plaintiff when there is a proven *bona fide* claim of infringement.[179]

The new provision includes a record preservation requirement. Pursuant to section 41.26 (1)(b), when a valid notice is received and the requisite fee paid, the access provider or host shall retain identity records of the person to whom the electronic location belongs.[180] They are required to hold the records for *six months* beginning on the day on which the notice of claimed infringement is received or, if the claimant commences proceedings relating to the claimed infringement and so notifies the person before the end of those six months, for *one year* after the day on which the person receives the notice of claimed infringement.[181]

Such a retention period has been criticized as privacy invasive.[182] Moreover, in *BMG*, the court refused to order the disclosure of identity information when there had been a delay of approximately six months between the copyright owners' investigation and the filing of the application in court. [183] Such a delay, the court held, gave rise to a risk that the iden-

---

174 *BMG Canada Inc. v. John Doe,* 2005 FCA 193, http://decisions.fca-caf.gc.ca/en/2005/2005fca193/2005fca193.html, [2005] 4 F.C.R. 81 [*BMG*].

175 *Norwich Pharmacal Co. v. Customs and Excise Comrs.,* [1974] A.C. 133 (H.L.), [1975] All E.R. 943 at 954 [*Norwich Pharmacal*].

176 *BMG,* above note 174.

177 *Norwich Pharmacal,* above note 175.

178 *BMG* above note 174 at para. 41.

179 *Ibid.*

180 Bill C-32, above note 5, s. 47. (See proposed s. 41.26 (1)(b).)

181 *Ibid.* (See proposed s. 41.26 (1)(b).)

182 Canada's Privacy Community, "Submission of Canada's Privacy Community" (13 Sept. 2009), www.ic.gc.ca/eic/site/008.nsf/eng/02670.html#footnote14 .

183 *BMG,* above note 174. This follows the approach of the UK House of Lords in *Norwich Pharmacal,* above note 175.

tity information could be inaccurate.[184] Since the use of inaccurate records could result in unjustified proceedings against innocent persons and an invasion of their privacy, failure to avoid delay could result in a court's refusal to order the release of identity information.[185]

A claimant may seek statutory damages for the failure of an ISP to fulfill its obligations under section 41.26(1) with respect to forwarding notices and retaining information in an amount that the court considers just in an amount not less than $5,000 and not more than $10,000.[186]

The NN provisions correct the most blatant problems associated with a NTD system. First, rather than force ISPs to make a (possibly inexpert) decision about copyright liability, the decision is left to the courts. As such, risk adverse ISPs might be less likely to err on the side of taking down allegedly infringing material at the expense of its customers and therefore reduce some of the detrimental effects from unfounded notices. Second, leaving the decision to take down content in the hands of the courts is consistent with the approach to hate propaganda and child pornography under the *Criminal Code*.[187] Third, by not requiring the automatic take down of content, the provision offers a less drastic response to a mere allegation of infringement, rather than a take down remedy which, with nothing more, is equivalent to a remedy for infringement. Finally, it does not presume that infringement problems always involve an intermediary host in a server-client relationship, leaving the door open for NN to apply more broadly to situations where ISP customers might be infringing using highly distributed peer to peer file sharing software.[188]

Bill C-32 does not, however, provide compensation from copyright owners to intermediaries for either their capital or operating expenditures resulting from the mandatory NN scheme which is, after all, for the benefit of copyright owners.[189] Furthermore, while the intent of Bill C-32 is to implement a NN system, it does not explicitly exempt an ISP from being found to have *authorized* infringement by failing to take down content once an allegation has been made. This differs from the United

184 *Ibid.* at para. 43.

185 *Ibid.* For discussion, see "Critical Privacy Issues in Canadian Copyright Reform" *IntellectualPrivacy.ca* (17 May 2006), www.cippic.ca/uploads/copyright-law-reform/Backgrouner-Copyright_and_Privacy.pdf .

186 Bill C-32, above note 5, s. 47. (See proposed s. 41.26(3).)

187 Sheryl Hamilton, above note 95, at 295-6.

188 "Entertainment Software Submission," above note 95.

189 "Submission of Bell, Rogers, Shaw and Telus," above note 4.

States *Digital Millennium Copyright Act* safe harbour approach[190] and may differ from the intent of Bill C-32. Under the safe harbour approach, once the conditions for a safe harbour are satisfied, including taking down allegedly infringing content, the safe harbour protects the service provider from copyright infringement liability.[191]

The difficulty can be explained by considering the immunity provision for hosts in the Bill. With respect to hosting, the new immunity is worded as follows:[192]

> 31.1(5) Subject to section (6), a person who, for the purpose of allowing the telecommunication of a work or other subject-matter through the Internet or another digital network, provides digital memory in which another person stores the work or other subject-matter does not, by virtue of that act alone, infringe copyright in the work or other subject-matter.

According to this provision, *hosting alone* does not infringe copyright in the hosted content. The difficulty is, however, that it does not make clear the legal effect of *a failure to take down* content that the host knows is infringing. Under proposed section 31.1(6) of the Bill, if the host knows of a court decision where the person who posted the work or other subject matter infringed copyright by posting it or by using the posted information, then the immunity under section 31.1(5) does not apply.[193] However, what if a copyright owner merely provides a notice (in the required form and content) alleging copyright infringement in relation to hosted information? Does the host authorize infringement by *omitting* to take down the content? Does the failure to take down in light of knowledge of infringing activity negate the host's status as a mere conduit? The immunity provision of the Bill should be clarified to ensure that, where a notice of alleged infringement has been received by an ISP in relation to some

---

190 *US Digital Millennium Copyright Act,* Pub. L. No. 10534, 112 Stat. 2860 (1998), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2281enr.txt.pdf [DMCA], s. 512.

191 Thus, in *Viacom International Inc. v. Youtube, Inc., Google, Inc. et al,* (USDC, Southern District of NY), 2010 (07 Civ. 2103 (LLS)), http://beckermanlegal.com/Documents/viacom_youtube_080702DecisionDiscoveryRulings.pdf , the court held, at 23, that when Youtube was given notices of infringement, it removed the material, protecting it from liability for contributory, vicarious and direct infringement.

192 Bill C-32, above note 5, s. 35. (See proposed s. 31.1(5).)

193 *Ibid.* (See proposed s. 31.1(6).)

subject matter, it is not liable for failure to prevent future infringement in relation to that subject matter.

d) Information Location Tools: Notice and Take Down?

Under the proposed section 41.25(1)(c) of the *Copyright Modernization Act*, search engine providers can receive notices of infringement from copyright owners in reference to works that they have cached.[194] Once a notice is received, search engines will be required to retain records in order to identify the alleged infringer.[195] Remedies for failure to comply with the retention requirements are the same as for other ISPs, namely, an award of damages between $5,000 and $10,000.[196] Under the proposed section 41.27(1),[197] Bill C-32 limits remedies against search engine providers who have been found to infringe by caching or communicating a cached copy to the public by telecommunication to injunctions, provided that the search provider has remained content neutral,[198] and provided that the search engine does not secondarily infringe under proposed section 27(2.3).[199]

The immunity from damages is limited under section 41.27(3) and this limitation provision appears to introduce a *de facto* notice and take down regime for search engines in cases where the infringing content has been taken down by its host.[200] Suppose, for instance, that a search engine has cached a copy of an infringing work from the Internet and that, as a result of receiving a notice, the infringing work has been taken down by its host. After that, the search engine provider is sent a notice (with the correct form and content) complaining of infringement by the search engine for reproduction of the work and for communicating the work to the public by telecommunication.

The validity of this complaint would be questionable, since under section 2.4(1)(b) of the *Copyright Act*, search engines do not communicate works to the public, at least not prior to the notice, so the notice would appear to be unfounded.[201] Further, on a broad interpretation of the common carrier principle, search engines do not make reproductions either. However, a number of counterarguments might be made at this point. First, it

194 Bill C-32, above note 5, s. 47. (See proposed s. 41.25(1)(c).)
195 *Ibid.* (See proposed s. 41.26(1)(b).)
196 *Ibid.* s. 48. (See proposed s. 41.26(3).)
197 *Ibid.* s. 47. (See proposed s. 41.27(1).)
198 *Ibid.* (See proposed s. 41.27(2).)
199 *Ibid.* (See proposed s. 41.27(4).)
200 *Ibid.* (See proposed s. 41.27(3).)
201 *Copyright Act*, above note 2, s. 2.4(1)(b).

might be argued that section 2.4(1)(b) of the *Copyright Act* does not apply to caching by search engines but only to caching by Internet access providers.[202] Second, it might be argued that, after a notice has been received by the search engine provider, it is no longer a neutral service and so it *is* communicating a work to the public by telecommunication and reproducing it. Third, it might be argued that, given the search engine's knowledge of a cached infringing reproduction and the ability to remove it, failure to remove it would be tantamount to authorizing communication and reproduction of it by others. The Bill needs to clarify these issues.

Under section 41.27(3), the immunity applies, in respect of reproductions made from the electronic location specified in the notice, *only* to infringements that occurred before the thirtieth day after the search engine provider receives the notice ("limitation day").[203] In other words, after the limitation day, a finding of infringement against the search engine provider for caching the infringing work or communicating to the public could result in an award of damages. In short, the search engine has 30 days to take down its cached work or risk infringement proceedings resulting in damages. This limitation provision introduces an unwarranted distinction between a NN system for hosts and a *de facto* NTD system for search engine providers since they are both generally automated and content neutral. It also bases the NTD system on the take down of content by a host for reasons that may be independent of the merit of an infringement claim, such as to obtain the protection of the safe harbour under section 512 of the *DMCA*.[204]

D. CONCLUSION

The intent of Bill C-32 is to modernize copyright law in light of new communications technology. Unfortunately, although the Bill resulted from a recent public consultation on copyright, the Government of Canada produced no comprehensive response paper explaining the rationale for its specific amendments. The Government's discussion in its *Improving Canada's Digital Advantage* and elsewhere suggests that its policy is rooted in a digital market philosophy in which copyright is a property right given as a reward for intellectual labour; that it is to primarily benefit copyright owners and, therefore, its dissemination by ISPs must be controlled for

202 *Ibid.*

203 Bill C-32, above note 5, s. 47. (See proposed s. 41.27(3).) Regulation may alter the limitation day.

204 *DMCA*, above note 190.

the benefit of copyright owners. In reality, this approach is rather antiquated in contrast to recent proposals to enable the free availability of copyrighted subject matter while compensating copyright owners through levies or compulsory licenses.

While the Government's discussion suggests that it aims to prevent online infringement by controlling the dissemination of copyrighted subject matter by ISPs, nevertheless, it introduces a strong immunity for innocent ISPs, rejects a GR system, and adds a form of secondary liability targeting those who intend to enable infringement that will be ineffective against peer to peer file sharing networks which have no centralized server. These choices might be explained by the fact that the Bill also seeks to target online infringement by *controlling the subject matter* itself. But, if the control of the subject matter through digital locks becomes widespread, it would be otiose and counterproductive to also control its dissemination. In the end, whether the control of subject matter is possible while also respecting the goals of copyright, privacy, free expression, and the rule of law remains to be seen.