Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation

JANE BAILEY*

I. INTRODUCTION

There exists an ongoing debate as to whether governments should attempt to regulate the Internet.[1] Those who argue that neither the Internet nor its content should be regulated often conflate the question as to whether, in principle, the Internet *should* be regulated with the related, but distinct question as to whether, in fact, the Internet *can* be regulated. As a result, many arguments against the application of law to the Internet and its content are premised on amoral bases.[2] Simply put, the argument is that if the medium defies regulation, you should not regulate it. While we should be concerned about enacting laws that are completely unenforceable laws have regularly been enacted without proof that they will regulate *perfectly*. Rather, the goal has generally been for laws to regulate *effectively*.[3] There is no principled reason to apply a different

* Assistant Professor in the University of Ottawa Faculty of Law, Common Law Section. Prior to commencing her position with the University, the author was an associate at Torys where she assisted as counsel for Sabina Citron, a complainant in the human rights tribunal proceedings relating to the "Zundelsite", discussed in detail below. The author wishes to thank her colleagues at Torys and at the University of Ottawa for their helpful suggestions relating to this paper. All inadequacies, however, are her own.

1 Dov Wisebrod, "Controlling the Uncontrollable: Regulating the Internet" (1995) 4 Media & Comms. L. Rev. 331; David Johnson and David Post, "Law and Borders—The Rise of Law in Cyberspace" (1996) 48 Stanford Law Rev. 1367; Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); Joel Reidenberg, "The Yahoo! Case and the International Democratization of the Internet" (April, 2001), on-line: Social Sciences Research Network <http://papers.ssrn.com/sol3?delivery.cfm/SSRN_ID267148_code010419520.pdf abstract id=267148> (date accessed: 20 August 2003).

2 Ian Kerr, "Mind Your Metaphors—An Examination of the Inefficacy Argument as a Reason Against Regulating On-line Conduct" in L.J. Pourciau, ed., *Ethics in Electronic Information in the Twenty-First Century* (West Lafayette, Indiana: Purdue University Press, 1993) 231.

3 Anglo-American law is replete with examples of laws that can never hope to eliminate acts philosophically determined to be morally wrong. Murder, rape and assault continue to

standard to the regulation of Internet content. In deciding whether to regulate Internet content we should ask two distinct questions: (i) *can* Internet content be regulated, and (ii) *should* Internet content be regulated. At a minimum, we should pay attention to the points in the regulatory decision-making process at which these two questions overlap.

Both questions have been addressed in Canada (in *Citron v. Zundel*[4] and, more recently, in *Schnell v. Machiavelli Enterprize Inc.*[5]) and in the U.S. (in *Reno v. A.C.L.U.*)[6] in the context of constitutional challenges to laws restricting certain types of Internet content. The decision makers in the two countries reached quite different conclusions regarding the role that the medium should play in determining whether content restrictions are consistent with freedom of expression. However, there are certain similarities in methodology between the two countries. The United States Supreme Court ("U.S.S.C.") spoke of the Internet as a monolithic whole, expressly adopting generalized metaphors as to what the Internet is.[7] The decisions of the Canadian Human Rights Tribunals ("C.H.R.T.")could also be read as accepting certain generalizations about the Internet, some of which while applicable to the application at issue in those cases (the World Wide Web ("WWW")), may not necessarily translate to other applications in future cases.

Adoption of general characterizations of the Internet as a whole in future cases risks obscuring the distinction between the two fundamental questions of whether the Internet *can* be regulated and whether it *should* be regulated through acceptance of assumptions that effectively mythologize the "Internet" as necessarily being a certain way—often leading to the erroneous conclusion that it cannot be regulated. Assuming that the Internet is necessarily a certain way precludes explicit consideration of factors that may affect the veracity of commonly accepted ideas about the nature of the Internet. As a result, it has been suggested that legal and policy issues relating to the Internet may be more

---

plague society despite laws against them, but we have not abandoned the laws because we have collectively accepted that there are certain acts that pose a sufficient threat to society or to individuals within society that we *should* attempt to regulate them, even if regulation will not eliminate them.

4 *Citron v. Zundel*, [2002] CHRD No. 1 (C.H.R.T.) (hereinafter "*Citron*").

5 *Schnell v. Machiavelli Associates Emprize Inc. and J. Micka*, [2002] CHRD No. 11 (C.H.R.T.) ("*Schnell*"). Since the writing of this paper, another decision relating to Internet hate propaganda has been released. See: *Warman v. Kyburz*, [2003] C.H.R.D. No. 18.

6 *Reno v. A.C.L.U.*, 117 S.Ct. 2329 (1997) (hereinafter '*Reno*').

7 Ian Kerr discusses the risk that the use of metaphors to describe technology can transform the value attached to technology. Rather than technology being seen as a human instrument, it becomes an end in itself and is valued as such: *supra* note 2 at 232–233.

effectively analyzed using a layered approach.[8] The layered methodology involves conceptualizing the Internet in layers, promoting explicit analysis of the intersection between legal values and the notional content, applications, and logical and physical elements that determine how the Internet is at any given point in time—thereby reducing the risk of implicit acceptance of generalizations about the Internet as a whole.

It is not suggested that use of a layered methodology would have affected the outcome in *Reno*, *Citron* or *Schnell*. Rather, it is suggested that a layered methodology that includes express examination of the role of Internet Service Providers ("ISPs") within the logical (or code) layer[9] makes explicit considerations not revealed in a monolithic approach or in a layered approach that focuses primarily on a single layer.[10] These considerations are key to distinguishing between and answering whether Internet content *can* and *should* be regulated. Further, consideration of certain aspects of the logical layer assists in illustrating how laws might be more effectively implemented, and suggests the possibility that the law of the least restrictive "connected" jurisdiction could come to dominate Internet content regulation.

The remainder of this paper is divided into four sections. Section II outlines in greater detail the decisions in *Reno*, *Citron* and *Schnell*. Section III describes the evolution of the layered methodology. Section IV applies the layered methodology to demonstrate that certain elements within the layers of the Internet intersect with key facets of existing U.S. and Canadian constitutional analyses, exposing the risk of decision-making based on generalizations about the Internet as a whole. Section V provides concluding remarks with respect to the potential contribution of the layered methodology in assessing whether Internet content *can* and *should* be regulated.

II. THE DECISIONS IN *RENO*, *CITRON* AND *SCHNELL*

Both U.S. and Canadian decision-makers have ruled on the degree to which the Internet, as a communications medium, affects the constitutional analysis of government-imposed restrictions on expression. Although decided against ma-

---

8 See for example: Timothy Wu, "Application-centred Internet Analysis" (1999) 85 Virginia L. Rev. 1163; Yochai Benkler, "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access" (2000) 52 Fed. Comm. L.J. 561; Lawrence Lessig, *supra* note 1 at 101. McTaggart has recently published a layered conceptual model that refines the model relied upon in the within paper. In addition to considering the physical, application, and content layers, his refined model reconceptualizes as the "operational layer" what is referred to in the within paper as the "logicallayer": Craig McTaggart, "A Layered Approach to Internet Legal Analysis" (2003) 48 McGill L.J. 571.

9 As suggested by McTaggart, *ibid.*

10 As suggested by Wu, *supra* note 8.

terially different constitutional backdrops that ultimately yielded different conclusions in each country, the *Reno, Citron* and *Schnell* decisions share similarities in their analytical approach. The U.S.S.C. in *Reno* failed to distinguish between the metaphor[11] of the Internet as a global marketplace of ideas and the layers of the Internet central to determining what the Internet *was, is* and *can be.*[12] The C.H.R.T.'s decisions could be interpreted to suggest two Internet metaphors. While the decisions in both *Citron* and *Schnell* refer to the "public" nature of the Internet, the two must be read in the context of the application at issue—the WWW. This characterization, while perfectly apt in relation to that application, cannot be generalized across Internet applications. Further, the *Citron* decision alludes to the myth that the Internet necessarily defies regulation—a suggestion which, if adopted in future cases, might lead to the inaccurate assumption that the only possible effect of legislation will be public denunciation of hate propaganda.

A. Reno v. A.C.L.U.

In *Reno* the U.S.S.C. considered whether provisions in the *Communications Decency Act* ("*CDA*")[13] aimed at protecting minors from indecent and patently offensive Internet content violated the First Amendment. The Court found that the provisions were an unjustified violation of freedom of expression. Its decision noted, in particular, that the provisions were over-broad since they also prevented people who have reached the age of majority from exercising their constitutional right of access to this type of content.[14] The conclusions of the Court, however, were not limited to an overbreadth analysis. The Court went on to comment upon the proper scope of constitutional protection for Internet communications more generally.

---

[11] Kerr, *supra* note 2.

[12] Lessig refers to the assumption that the Internet "is" a certain way as the "is-ism". He identifies that the way the Internet "is" at any point in time will not necessarily continue into the future. Decision-making about legal regulations, therefore, should explicitly recognize the potential impact of changes in Internet architecture, markets and norms on the continuing precedential value of decisions that are based on the state of technology at the time. See: Lessig, *supra* note 1 at 166–167.

[13] *Communications Decency Act (1996)*, 47 U.S.C. §§223(a) to (h).

[14] In fact, the U.S.S.C.'s conclusion in this regard was premised on the faulty assumption that the Internet necessarily facilitates anonymous communication. As discussed below, technological innovation increasingly makes possible identifying users based on their identity, age, and geographic location. See: "Geography and the Internet: Putting it in its place", The Economist (August 9, 2001), on-line: The Economist <http://www.economist.com/opinion/display story.cfm?story_id=729808> (date accessed: 5 July 2003).

While the Court recognized in the fact section of its judgment that there were different modalities of Internet use, such as e-mail and web browsing, material differences between these applications were not factored into the majority's fundamental conclusions. Rather, these conclusions were informed by a series of broad generalizations about the Internet. The Court characterized the Internet as a global communications medium leading to a "dramatic expansion of the marketplace of ideas" with a range of content as "diverse as human thought".[15] Other generalizations about the Internet led to similar conclusions that the Internet facilitated equal, global diversity, and participation, and that the Internet was not invasive in that users "pulled" content to themselves and only infrequently were confronted with uninvited content.[16] Based on these generalizations, the U.S.S.C. concluded that restrictions on Internet expression would be subject to strict constitutional scrutiny.[17]

B. C.H.R.T. Decisions

1. Citron v. Zundel

One of the issues to be determined in *Citron* was whether s.13(1) of the *Canadian Human Rights Act* ("CHRA"),[18] when applied to Internet communication, violated the freedom of expression guarantee in the *Canadian Charter of Rights and Freedoms*. Specifically, the issue was whether application of a provision prohibiting the telephonic communication of hate speech to the website known as the Zundelsite violated the *Charter*. A two-member C.H.R.T. panel found restriction of the website to be consistent with the *Charter*. In reaching that conclusion, the C.H.R.T. recognized many of the constituent elements comprising the Internet. However, its ultimate conclusion about the public nature of the Internet must be read in light of the application at issue in the case and cannot be assumed to apply equally to all other applications apart from the WWW. In this regard, the C.H.R.T., noting the Internet's global nature, held:

> The pervasiveness of the Internet persuades us that this mode of communicating hate messages is most pernicious. ... a public means of communication is used, yet the listener enjoys direct, seemingly personal contact in relative privacy.[19]

---

15 *Reno*, *supra* note 6 at 2335-6, 2340.

16 *Ibid.* at 2343.

17 Other decisions by U.S. courts reached the same conclusion, characterizing the Internet as "a never-ending worldwide conversation" (*Reno v. A.C.L.U.*, 929 F. Supp. 824 (Ed.PA. 1996)), or as "a brave new world of free speech" (*Blumenthal v. Drudge*, 992 F. Supp. 44, 48 n. 7).

18 *Canadian Human Rights Act*, R.S.C. 1985, c. H-6 (hereinafter "CHRA").

19 *Citron*, *supra* note 4 at para. 95.

The C.H.R.T.'s constitutional analysis was guided by prior decisions of the Supreme Court of Canada ("SCC") in *Keegstra*[20] and *Taylor*.[21] The SCC held in *Taylor* that the *CHRA* provision at issue in *Citron* violated freedom of expression under s. 2(b) of the *Charter*, but constituted a justifiable limit pursuant to s. 1. The Court in *Taylor*, however, was dealing with the question of constitutionality in the context of hate propagation through pre-recorded messages disseminated from a telephone answering machine, rather than via the Internet. The C.H.R.T.'s analysis therefore focused on whether there was something sufficiently different about the Internet that would change the SCC's conclusion of constitutionality in *Taylor*.

After concluding that the provision was constitutional and that the respondent had violated the provision, the C.H.R.T. issued a "cease and desist" order against him and those acting in concert with him. In making its order, the Tribunal's decision could be taken to suggest another Internet metaphor—that the Internet necessarily defies territorial regulation. Specifically, the C.H.R.T. held that, although its order may have no effect in terms of eliminating the material in question from the WWW, given mirroring[22] technology, the order would have symbolic value by publicly denouncing this type of expression.[23] If broadly accepted in future cases, this approach could lead to the unnecessary assumption that the effect of orders under the *CHRA* will necessarily be limited to solely to denunciation.

2. Schnell v. Machiavelli

The C.H.R.T. panel in *Schnell* confronted similar issues to those involved in *Citron*, but in relation to hate propaganda targeting gays and lesbians. The C.H.R.T. found that the respondents, who were involved in the creation and dissemination of the anti-gay and lesbian content in issue through the website "citizenresearchinst.com", had violated ss. 13(1) of the *CHRA* by acting in concert to communicate messages that were likely to expose individuals to hatred or contempt on the basis of their sexual orientation. The Tribunal further held that the provision was consistent with the *Charter*'s freedom of expression guar-

---

20 *R. v. Keegstra*, [1990] 3 S.C.R. 697 (hereinafter "*Keegstra*").

21 *Canadian Human Rights Commission v. Taylor*, [1990] 3 S.C.R. 892 (hereinafter "*Taylor*") ; *Keegstra*, *ibid.*

22 Where a website is ordered to remove content in one jurisdiction, the content of that site can be copied to a server in another jurisdiction where the content restriction cannot be enforced. For a further description of the uses of mirroring to evade content restrictions, see: Joy Shaw, "Internet Censorship in China" (2002) U.S.C. Annenberg Online Journalism Review, online: University of Southern California <http://www.ojr.org/ojr/business/1017967553.php> (date accessed: 20 August, 2003.

23 *Citron*, *supra* note 4 at paras. 295, 297.

antee, even as applied to the Internet. In reaching this conclusion, it relied on the SCC's conclusion in *Taylor* that the telephone was ideally suited to spreading hate propaganda. In this regard, the C.H.R.T. found that:

> [I]f the telephone is ideally suited to spread prejudicial ideas, the Internet is even better positioned. It is a very public form of communication, inexpensive, easily accessed, and can communicate many messages simultaneously and instantaneously to a worldwide audience.[24]

As noted above, in relation to *Citron*, it will be important in future cases to recognize that this finding as to the public nature of the Internet will not necessarily apply equally across applications, although it clearly applied to the websites in issue. Unlike the situation in *Citron*, where the respondent left the jurisdiction, the respondents in *Schnell* appear to have remained in Canada. Perhaps as a result of this factual distinction between the cases, the C.H.R.T. in *Schnell* issued a cease and desist order against the respondents without alluding to the myth of the regulation-defying "nature" of the Internet.

C. Similarities Between *Reno, Citron,* and *Schnell*

The ultimate conclusions in *Reno*, *Citron*, and *Schnell* reflect, at least in part, material differences between the U.S. and Canada with respect to restricting expression. While U.S. courts frequently hold that restrictions on certain forms of expression such as pornography and hate propaganda violate the First Amendment,[25] the SCC has tended toward an equality-based approach pursuant to which restrictions on these forms of expression stand a greater chance of surviving constitutional scrutiny.[26]

Despite the difference in result, one or more of three generalizations about the Internet arise in each of these decisions: (i) that the Internet as a whole can be categorized as public or private in nature; (ii) that the Internet defies territorial regulation; and (iii) that the Internet necessarily facilitates a global conversation.

---

[24] *Schnell*, *supra* note 5 at para. 156.

[25] See for example: *Miller v. U.S.*, 413 U.S. 15 (1973) ("*Miller*") (limiting restrictions to *obscenity* only), *R.A.V. v. St. Paul*, 112 S.Ct. 2538 (1992) at 2542-2544 ("R.A.V.") (hate speech). Of course, this is not universally true. For example, the US courts have approved restrictions on obscenity in circumstances where it is not clear that the SCC, using its equality-based approach would have done so. See for example: *Skywalker Records Inc. v. Navarro*, 742 F.Supp.638 (S.D. Fla. 1990).

[26] See for example: *R. v. Sharpe*, [2001] 1 S.C.R. 45 (*Sharpe*) (re: child pornography) and *Taylor*, *supra* note 21 and *Keegstra*, *supra* note 20 (re: hate propaganda). Again, this is not universally true. For example, in *Zundel* the SCC struck down a *Criminal Code* provision used to restrict hate propaganda on the basis that it was not sufficiently tailored to minimize the impairment of the *Charter*'s freedom of expression guarantee: *R. v. Zundel*, [1992] 2 S.C.R. 731 ("*Zundel*").

Future acceptance of these generalizations in other cases could produce at least three substantive consequences. First, it could mask the reality that the Internet can change if certain elements within its layers change, with the risk that decisions based on generalizations will quickly become out-dated, even if the generalizations are relatively accurate at a given point in time.[27] Second, elements of the Internet that intersect directly with important public values reflected in existing constitutional analyses in both countries might be obscured. These issues are directly relevant to whether Internet content *should* be regulated in order to preserve existing constitutional values. Third, any assumption that the Internet defies territorial regulation risks missing the opportunity for even more effective regulation by failing to explicitly consider certain Internet elements making Internet content increasingly regulable.[28]

III. THE LAYERED METHODOLOGY

The layered methodology is an evolving tool designed to assist in organizing the analysis of Internet-related legal and policy issues. Timothy Wu explicitly articulated the advantages of the layered methodology and identified the shortcomings of the monolithic approach in *Reno*. He argued that First Amendment issues could not be adequately resolved if the Internet is assumed to be *one* particular thing. Wu postulated a two-layer analysis, with the second layer broken into three sub-layers. The applications layer focuses on the uses that can be made of the Internet (e.g. e-mail, web browsing, etc.). The transport layer is divided into three sub-layers—transport protocol (the agreed-upon format for routing traffic on the Internet), network protocol (the agreed-upon format by which networks are connected on the Internet), and link protocol (the agreed-upon format by which users establish their link to the Internet).[29]

Wu suggested that the applications layer was key to analysing First Amendment issues. In this regard, he noted established U.S. constitutional reasoning[30] that content restrictions on media invading the privacy of an unsuspecting listener will be more easily justified than restrictions on non-invasive

---

27 In fairness to the U.S.S.C., the dissenting justices, per Day O'Connor J., did recognize that technological change might facilitate labeling and filtering that would make it possible to restrict only minors' access to the material in question: *Reno*, *supra* note 6 at 2353-2354.

28 Lessig powerfully illustrates, for example, the degree to which intellectual property rights can be *too* effectively regulated, given key aspects of the Internet's architecture—an architecture not necessarily of freedom, but with equal potential for control: *The Future of Ideas* (New York: Random House Inc., 2001).

29 Wu, *supra* note 8 at 1191.

30 See for example: *Gormley v. Director, Conn. State Dept. of Probation*, 632 F. 2d. 938 at 942 (2d. Cir. 1980); *Frisby v. Schultz*, 487 U.S. 474 at 484–485 (1988).

media.[31] Wu noted that the U.S.S.C.'s conclusions in *Reno* that the Internet is non-invasive and that Internet content is only rarely imposed on unsuspecting users resulted from the Court's failure to consider the differences among Internet applications.[32] On this basis, he suggested that the applications layer would be the most significant in Internet-related freedom of expression analysis.

Other Internet scholars also rely on layered methodologies in analysing Internet-related legal and policy issues.[33] Lessig has powerfully illustrated the degree to which control over the logical layer—the computer code underlying the hardware and software comprising the Internet—could influence the content available through the Internet. Further, Benkler and Lessig posited that freedom of expression was not necessarily best served through the absence of regulation, but through a layered approach to regulation designed to facilitate the ideal of an unmediated conversation of the many with the many.[34] Employed in this sense, a layered approach offers the opportunity to explicitly *assess* the degree to which any particular regulatory scheme serves the ideal of a global, diverse, and equal information exchange through an unmediated network, rather than *assuming* it as the U.S.S.C. did in *Reno*.

The work of McTaggart suggests a four-layer methodology focusing on content, applications, logical and physical layers.[35] The content layer relates to the data and transactions actually available on the Internet. The applications layer parallels that proposed by Wu—focusing on the software that facilitates use of the Internet. The logical layer relates to the technical functions that allow for the transmission of packets between networks. The physical layer encompasses the media over which the logical layer operates—including the telecommunications network and the computer hardware through which, among other things, users establish their connection to the Internet. Contrary to Wu's suggestion, McTaggart has suggested that the logical layer, which is critical to connectivity, could play a central role in the analysis of Internet-related legal or policy issues.[36]

Layered methodologies are preferable to a monolithic approach because they assist in conceptualizing the Internet in component parts, limiting the temptation to rely on mythical generalizations and facilitating explicit distinc-

---

31 Wu, *supra* note 8.

32 *Ibid.* at 1167–1168.

33 Benkler, *supra* note 8; Lessig, *supra* note 1.

34 Benkler, *supra* note 8 at 565; Lessig, *supra* note 1.

35 McTaggart has pointed out that Benkler and Lessig's "logical" or "code" layer conflates applications with the protocols that facilitate transmission, thereby suggesting the need for a fourth layer separating these two aspects: *supra* note 8 at 5.

36 McTaggart, *supra* note 8 at 4.

tions between what the Internet was, is and can be. Part IV will use the four-layer methodology to explore the explicit connection between each layer and U.S. and Canadian constitutional analyses of content regulation. Not only the applications layer, but the content, logical and physical layers intersect with key aspects of the U.S. and Canadian analyses and, on a broader level, play an important role in determining whether the policy of the least restrictive jurisdiction will dominate Internet content.

IV. INTERSECTION OF INTERNET LAYERS WITH U.S. AND CANADIAN CONSTITUTIONAL ANALYSES OF CONTENT REGULATION

Each layer in the four-layer approach bears directly on one or more of the "marketplace of ideas" concept, privacy commitments and efficacy concerns underlying freedom of expression analysis in the U.S. and in Canada.

A. The Content Layer

The content layer comprises the material that users can get from the Internet—everything from on-line gambling to recipes to pornography to the text of international human rights conventions. Internet content intersects with U.S. and Canadian constitutional analyses in at least two ways. First, the type of content at issue will affect the degree to which its restriction will be scrutinized. Second, the breadth of content available intersects with the "marketplace of ideas" concept underlying freedom of expression analyses in both countries.

1. The type of content at issue

The type of content at issue will influence both U.S. and Canadian constitutional analyses of content regulation. While it will be easier to justify restrictions on content not contributing to the values underlying freedom of expression (such as the search for truth) in both the U.S. and Canada, the two countries often take different views as to which types of expression actually contribute.[37] U.S. courts have determined that certain categories of speech, such as libel, obscenity and "fighting words", are excluded from constitutional protec-

---

[37] Despite a not insignificant body of rhetoric surrounding the First Amendment and the degree to which it protects "free" expression, the fact is that U.S. courts have approved restrictions on many types of expression. Ironically, while many U.S. commentators saw the enforcement of a French court order relating to hate speech as a death knell for freedom of expression, very few commented upon the restrictions effectively imposed by the U.S. court in relation to webcasting in Canada. For further commentary on this issue, see: Reidenberg, *supra* note 1; Thoumyre, Lionel, "The legal implications in Yahoo! Inc. Nazi memorabilia dispute: an interview with Michael Geist", on-line: Juriscom < http://www.juriscom.net/en/uni/doc/yahoo/geist.htm> (date accessed: 20 August 2003).

tion,[38] while creative freedoms restricted through copyright and patent protection tend to receive minimal First Amendment protection.[39] In Canada, the SCC has avoided a categorical approach, holding that the *Charter* freedom of expression guarantee protects *prima facie* all non-violent attempts to convey meaning, subject to the imposition of reasonable limits.[40] The SCC has determined that limits on content such as pornography and hate propaganda (as particularly defined in the *Criminal Code*[41] and in the *CHRA*) are more easily justified because that content lies far from the core values underlying freedom of expression[42] and has suggested that restrictions imposed on creative freedoms through intellectual property regimes should be carefully scrutinized.[43]

The type of content at issue can be expected to continue to affect constitutional analyses of regulations imposed on Internet expression, although the U.S. and Canada are unlikely to approach this issue from a consistent perspective.

2. The role of "marketplace" diversity in U.S. and Canadian constitutional analyses of content regulation

Both U.S. and Canadian constitutional analyses of content regulation are influenced by the concept of the "marketplace of ideas".[44] Relying on this concept, courts in the two countries have concluded that the search for truth is best served in a marketplace where the widest possible variety of ideas freely compete for consumer acceptance.[45] While the jurisprudence in both countries fre-

---

38 See: *New York Times v. Sullivan* 376 U.S. 254 (1964) (re: libel); *Chaplinsky v. New Hampshire* 315 U.S. 568 (1942) (re: "fighting words"); and *Miller*, *supra* note 25 (re: obscenity). However, at least one recent decision suggests that regulation specifically aimed at even these types of content will still be strictly scrutinized under the First Amendment: *R.A.V.*, *supra* note 25.

39 Lessig, *supra* note 1.

40 *Irwin Toy Limited v. Quebec (Attorney General)*, [1989] 1 S.C.R. at 968.

41 R.S.C. 1985, c. C-46 as am.

42 *Keegstra*, *supra* note 20; *Sharpe*, *supra* note 26; *Thomson Newspapers Co. v. Canada*, [1998] 1 S.C.R. 877, at paras. 90–92.

43 See: *Théberge v. Galerie d'Art du Petit Champlain inc.*, [2002] 2 S.C.R. 336 (re: intellectual property).

44 In the U.S., see for example: *R.A.V.*, *supra* note 25; *Schenck v. United States*, 249 U.S. 47 (1919), per Holmes J. In Canada, see for example: *Edmonton Journal v. Alberta (Attorney General)*, [1989] 2 S.C.R. 1326; *Zundel*, *supra* note 26. While I have questioned the viability of the marketplace model in "Private Regulations & Public Policy: Toward Effective Restriction of Internet hate Propaganda" (2003) [unpublished, copy available from the author], the purpose of this part of the paper is simply to discuss how that concept maps to the internet.

45 Reidenberg, *supra* note 1.

quently refers rhetorically to the concept of a laissez-faire marketplace of ideas, U.S. and Canadian courts have found certain government limitations on that marketplace to be constitutional—albeit based on different values in each country.[46]

There is arguably at least one principled difference between the approaches of the two countries in relation to the "marketplace" concept. The U.S. approach is generally underlain by significant skepticism of the ability of government regulation to *enhance* liberty.[47] It frequently focuses on responding speech as the best remedy for the harmful effects of certain expression. In contrast, the SCC has explicitly recognized that government regulation *can* facilitate liberty and freedom by eliminating barriers to entry for those targeted by certain types of expression that cannot adequately be addressed by "more speech".[48] In this way, although marketplace diversity will be important in analysing content regulation in both countries, the degree to which it will influence the result is likely to be affected by whether responding expression is considered to effectively ameliorate the harmful effects of the content in issue.

The sheer quantity of and ease of access to content on the Internet, relative to other mass media, appears to have been an influential factor in the U.S.S.C.'s decision in *Reno*. Having found that the Internet is accessible around the globe and provides content as "diverse as the human mind", the U.S.S.C. determined that government-imposed content regulation in that space should be strictly scrutinized.[49] In other words, the U.S.S.C. assumed a global diversity of ideas and participants in Internet communication would generate a robust competition of ideas, circumscribing the need for government intervention.[50] Consistent with the Canadian approach, the C.H.R.T.'s decision in *Citron* focuses on the

---

46 For example, the U.S.S.C. has said that the First Amendment generally protects hate speech, while Canadian jurisprudence indicates hate speech can be constitutionally regulated. See: *R.A.V.*, *supra* note 25; *Taylor*, *supra* note 21; and *Keegstra*, *supra* note 20.

47 Reidenberg, *supra* note 1; Lessig, *supra* note 1 at 5.

48 *Keegstra*, *supra* note 20 (re: hate propaganda); *R. v. Butler*, [1992] 1 S.C.R. 452 (re: pornography). This approach is not dissimilar to Lessig and Lemley's suggestion that the exercise of anti-trust authority to limit certain economic actors from abusing their dominant position might in fact enhance competition and freedom overall: Lawrence Lessig and Mark Lemley "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era" (2001) 48 UCLA Law Review 925.

49 *Reno*, *supra* note 6 at 2351.

50 Again, this is not universally true in application. The nature of the content will also affect the decision. For example, although the importance of the "marketplace of ideas" is stressed in relation to hate propaganda (see: *R.A.V.*, *supra* note 25; it may figure less prominently in copyright-related decisions, even in relation to the Internet, (see: *Universal City Studios v. Reimerdes*, 82 F.Supp.2d 211 (S.D.N.Y. 2000)).

degree to which certain types of expression in an unregulated marketplace may reduce competition by silencing members of target groups.[51]

In this way, the content layer may affect U.S. and Canadian constitutional analyses quite differently, with perhaps a greater hesitancy in the U.S. to approve of restrictions in the context of an abundant marketplace. An explicit examination of other layers reveals potential barriers to participation that suggest the need for caution in assuming that the Internet actually models the laissez-faire marketplace ideal—even if one were to accept that model as "ideal". These barriers, which may affect the diversity of content and equality of Internet participants, will be explored further in the context of the logical and physical layers.

B. The Applications Layer

Analysis of the applications layer speaks directly to generalized categorization of the Internet as distinctly public or private. The degree to which the Internet is public or private is significant to U.S. and Canadian constitutional analyses of content regulation in at least two ways. Both the privacy-invasiveness of particular Internet applications and the degree to which any particular use of an application creates a private sphere of communication are likely to affect the justifiability of content restrictions relating to those applications.

1. U.S. and Canadian values relating to privacy

The public or private nature of any particular form of communication affects both U.S. and Canadian constitutional analyses of content restrictions. In both countries, the constitutional justifiability of a content restriction will be influenced, at least in part, by whether the objectives of the restriction outweigh its negative effect on other constitutional values, including security from government intrusion in private activities. Simply put, the more private the communication, the more difficult it will be to justify regulating its content. Privacy issues manifest themselves in at least two different forms in this context.

First, all else being equal, it is likely to be easier to justify restrictions on applications that "push" on unsuspecting listeners. In these circumstances, content restrictions undermine freedom of expression, but at the same time serve privacy interests by protecting unsuspecting listeners from undue invasion of their privacy by other private actors.[52] Second, all else being equal, it is likely to

---

[51] *Citron*, *supra* note 4 at paras. 59–60. It may be that the relevance of "diversity" in the marketplace depends on the nature of the content at issue. It might be argued that the harms associated with certain types of expression are not alleviated by the fact that they are competing with a wide diversity of ideas within the marketplace. To this extent, a broader marketplace will not necessarily undermine the justifiability of restrictions on certain types of expression.

[52] Wu, *supra* note 8; *Keegstra*, *supra* note 20 at 763.

be easier to justify restrictions on applications making content "publicly" available than those involving consensual private exchange because restrictions on publicly available content, are less likely to trigger individual privacy concerns.[53]

The justifiability of the restriction should depend not only on the application in use, but also on the nature of the content restricted and the particular use made of the application in any given circumstance.

2.Privacy invasiveness of the application

Where, as Wu argued, an application delivers content only as the result of steps taken by the user to "pull" that content toward him or herself, government cannot justify restrictions on the basis that they protect listeners from uninvited intrusion. As such, Wu suggested that content regulations on "push" applications should be more easily justified than restrictions imposed on "pull" applications. In support of his argument, Wu cited the powerful privacy-invasive example of "spam"—the unsolicited bulk e-mail sent unbidden often to thousands (and even millions) of recipients.[54] Using this example, Wu criticized the U.S.S.C.'s conclusion that the "Internet" is non-invasive—powerfully demonstrating that the degree of invasiveness can be heavily influenced by the application in use.

As Wu acknowledged, however the application itself provides only a rough guide with respect to privacy invasiveness. The inquiry should be further supplemented in two respects—one relating to the nature of the content at issue and the other relating to the particular use of the application.

First, both U.S. and Canadian courts have determined that restrictions on certain content will be justifiable, regardless of whether the content is "pulled" by the listener or exchanged consensually in relatively private circumstances. In the U.S., for example, the First Amendment does not protect "obscenity", regardless of the circumstances in which this type of content is communicated.[55] In Canada, ss. 2(b) of the *Charter* does not generally protect either the dissemination or the private possession of child pornography.[56] In these and other circumstances, the U.S.S.C. and the SCC have found that the government objective of limiting the risk of social harms arising from these types of content

---

[53] Further, in Canada, in the context of socially harmful content, restrictions relating to publicly available content ought to be more easily justified since the expanded scope of the potential audience escalates the risk of widespread adoption of socially harmful attitudes associated with that content: *Citron*, *supra* note 4 at paras. 59–60. This concept has been soundly rejected in the U.S., see, for example: *Ashcroft v. Free Speech Coalition* 122 S.Ct. 1389 (2002).

[54] Wu, *supra* note 8 at 1176.

[55] *Miller*, *supra* note 25.

[56] *Sharpe*, *supra* note 26.

and/or the minimal value of the expression in question outweigh privacy concerns. These value-based commitments should not be undermined, in the Internet context, by the nature of the application in issue.

Second, just as it was incorrect for the U.S.S.C. to state that the Internet is non-invasive, it would be equally incorrect to characterize any particular application either as privacy invasive or non-invasive. While the push/pull analysis suggested by Wu does assist in making generalized comparisons between applications, it does not take into account the impact of particular uses of applications. For example, it may be more difficult to say that content was "pushed" on an e-mail recipient where that recipient "invited" a responding e-mail in an earlier message or where the recipient took an active step to decode an encrypted e-mail.[57] The characterization of e-mail as a "push" application may be further undermined in the context of mailing lists where a recipient takes the active step of subscribing to the list.[58] Similarly, it will not always be accurate to characterize WWW browsing as a true "pull" application. As Wu acknowledged, it may be more difficult to suggest that a recipient "pulled" content where a search term yields unexpected results.[59]

Therefore, the application itself is not necessarily determinative of the degree to which content can be accurately characterized as invading the recipient's privacy. Other factors relating to the particular use of an application should be considered in determining whether content can be fairly characterized as "pushed" on or "pulled" in by a recipient in any given circumstance. The analysis should focus on whether the user could reasonably have expected to be exposed to the content in issue, considering factors such as whether the user "invited" certain content through prior contact with the sender or took active

---

[57] Encryption involves the translation of data into a secret code. In order to read an encrypted message, you must possess the virtual "key" or a password. See: on-line: http://www.webopedia.com/TERM/e/ encryption.html (date accessed: 20 August 2003).

[58] A mailing list is a list of e-mail addresses identified by a single name. When an e-mail is sent to that address, it is automatically delivered to all addresses on the list. See: on-line: http://www.webopedia.com/ TERM/m/mailing_list.html (date accessed: 20 August 2003).

[59] The Federal Trade Commission announced in September 2001 that it would take action against website owners engaged in the practice of "mousetrapping" (use of typo variants of popular domain names in order to dupe unsuspecting web surfers into visiting pornographic or on-line gambling sites): Brian Krebs, "FTC Cracks Down on Porn, Gambling Site 'Mousetrapping'" (26 September 2001) Newsbytes, on-line: http://www.newsbytes.com/news/ 01/170531 .html [copy available from the author]. Further, it is notable that some websites employ "automatic" hyperlinks that, without "consent" of the user instruct his or her browser, on accessing the first website, to automatically download a file from a second site: *SOCAN Statement of Royalties, Public Performance of Musical Works 1996, 1997, 1998 (Tariff 22, Internet (Re)* (1999), 1 C.P.R. (4th) 417 at 438 (Copyright Board), aff'd. in material part, *Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers*, 2001 F.C.A. 166, ("SOCAN").

steps, such as using decryption technologies or subscribing to participate in communications through a particular application.[60]

3. Private spheres of communication

Canadian constitutional analysis of content regulation, in particular, works toward striking a balance between minimizing the harmful risks associated with particular content and minimizing government intrusion in truly private spheres of communication, thought, and conscience.[61] Restrictions on truly private spheres are likely to be more difficult to justify, particularly where they limit expression unintended for public dissemination and where creation of the content did not itself occasion harm.[62]

In light of the variation among applications illustrated by Wu, it would be an over-generalization to conclude that the Internet is a public means of communication, although certain Internet applications, such as the WWW, certainly are. The degree to which Internet expression may be conceived of as private or public will be affected by a number of factors—including the application chosen. However, just as it has been suggested that it is unhelpful to categorize applications as privacy-invasive or non-invasive, it would be similarly unhelpful to categorize them as private or public in nature. Rather, one application might be considered more private than another along a continuum from most public to most private, with variations depending upon the particular use to which it is put in any given situation.[63] Technologically neutral factors might be considered, including: the number of participants in the communication in issue, the diversity of persons other than the participants who can access the communication, the depth of attachment of the participants to one another, and the purpose for which the communication is made. As these criteria coalesce toward an

---

60 Similar factors were taken into account by the Human Rights and Equal Opportunity Commission ("HREOC") of Australia in determining that the website of Frederick Toben violated the incitement of racial hatred provisions in its *Racial Discrimination Act, 1975*. See: Michelle Hannon, "Racial Hatred Provisions Applied to the Internet" (28 March 2002), on-line: Gilbert + Tobin < http://www.gtlaw.com.au/flash/indexjsp?c=splash.html?&s=news.jsp&p=o&e=f&t=GILBERT+and+TOBIN&a=false > (date accessed: 20 August 2003).

61 *Sharpe*, *supra* note 26 at para. 26; *Taylor*, *supra* note 21 at 937–939.

62 *Sharpe*, *ibid.* U.S. constitutional analysis also reflects the concern that limitations on expression may undermine freedom of thought and conscience. See: *Ashcroft*, *supra* note 53.

63 That being said, certain applications, such as posting on the WWW, are likely to consistently fall at the public end of the spectrum. This is primarily a function of the ease with which WWW content is accessible to millions of people around the world, whether or not they are familiar with the poster. In fact, the SCC recently noted the similarity between posting on the WWW and posting messages on public billboards. See: *Guignard v. City of Saint-Hyacinthe*, [2002] 1 S.C.R. 472.

intimate, personal conversation between friends or acquaintances, content regulation in relation to that use of the application can be expected to be more strictly scrutinized.[64] In contrast, as these criteria move toward a broad-ranging communication of messages to anyone with an Internet connection, all else being equal, content regulation with respect to use of the application will likely be less strictly scrutinized.

C. The Logical Layer

Analysis of the three elements of the logical layer—management of centralized resources and functions, standards and protocols, and ISPs—exposes the twin myths that the Internet necessarily facilitates a diverse global conversation and that the Internet necessarily defies territorially based regulation. These elements of the logical layer therefore relate to Canadian and U.S. constitutional analyses in at least two ways. First, they affect the diversity of the Internet as a marketplace of ideas. Second, they raise issues as to the efficacy of territorially based regulation—a factor particularly relevant to Canadian constitutional analysis. In each instance, distinguishing between pre-existing "ideals"[65] about the Internet and the way in which the logical layer has developed reveals the risk inherent in decision-making based on uncritical acceptance of generalizations about the Internet as a whole.

1. Diversity of the internet marketplace

i. The Ideal Logical layer

If Internet addressing, standards and protocols, and ISPs facilitated a diverse marketplace of ideas, then U.S., and to some extent, Canadian courts would be likely to scrutinize restrictions on Internet content more strictly.[66]

The centralized resources and functions of the Internet's logical layer include the addressing function. Currently, each computer is assigned a unique Internet Protocol ("IP") address from a pool of addresses overseen by a central

---

[64] Both the SCC and the Australian H.R.E.D.C. have considered these type of factors in relation to privacy-related issues: *Gould v. Yukon Order of Pioneers*, [1996] 1 S.C.R. 571; Michelle Hannon, *supra* note 60. We should not lose sight, however of the possibility that private, consensual consumption of socially harmful expression may, in fact, create a significant risk of harmful behaviour, even though it may not reach a widespread audience. As Sunstein has argued, intimate groups of like-minded people may reinforce one another's previously held biases, fomenting adoption of even more extreme positions: Cass Sunstein, *Republic.com* (New Jersey: Princeton University Press, 2001).

[65] In this section, the term "ideal" accepts, for purposes of argument, a more libertarian "ideal" of "free" expression—that is, expression free from centralized restriction.

[66] However, as noted above, the diversity of the marketplace is unlikely to affect the justifiability of restrictions on certain types of expression that U.S. and Canadian courts have previously determined to be socially harmful and/or unworthy of constitutional protection.

authority—the Internet Corporation for Assigned Numbers and Names. Users do not enter an IP address to transmit information. Instead, they enter a "domain name" that is easier to remember, but does not necessarily reveal the identity of the person or organization to whom it belongs. The domain name is translated back to the IP address through the Domain Name System in order to transport the data to its intended destination.[67] Ideally, the unique numeric identifier, rather than specific user identifying information, would form the basis for data transmission on the Internet.

The Transmission Control Protocol and Internet Protocol ("TCP/IP") define the basic architecture supporting the Internet. While networks and users could choose to adopt other protocols, the effect would be self-exclusion from the Internet.[68] TCP opens and closes the connections necessary to exchange information. It is not designed to "understand" the message being sent. Rather, its only task is to ensure that the message has been sent.[69] These simple and accessible protocols facilitate end-to-end design[70], non-discriminatory packet switching,[71] and potentially global connectivity through a multi-jurisdictional network of networks,[72] maximizing the potential for accessibility, participation, and creativity for anyone with a connection to the Internet. Further, TCP/IP can facilitate anonymous expression, to the extent they operate on the basis of information that does not necessarily identify the user. Anonymity might be ex-

---

67 *SOCAN*, *supra* note 59 at 430.

68 McTaggart, *supra* note 8 at 17.

69 *SOCAN*, *supra* note 59 at 432.

70 End-to-end design refers to a communications medium with a "stupid" network and intelligent terminals at either end. This particular type of structure ensures maximum functionality at the ends of the network, rather than placing control over functionality in the hands of the owner of the network. Timothy Denton and Francois Menard, "A Paradigm Shift for the Stupid Network" (15 June 2000) at 7, online: www.tmdenton.com/pdffiles/A_Paradigm_Shift_For_The_Stupid_Network.pdf> (date accessed: 20 August 2003).

71 Packet switching or packet routing in the Internet context refers to the fact that data is transmitted over the network in packets. For example, an email message will be broken down into packets, each containing the IP address to which the message is to be sent. The packets will be independently routed along the network (not necessarily taking the same route) until they reach their destination, at which time they are reassembled into a readable message. Federal Communications Commission, *Digital Tornado: The Internet and Telecommunications Policy* by Kevin Werbach (Washington: Office of Plans and Policy Working Paper Series No. 29, 1997 at 17.

72 The Internet has been described as a "network of networks." Networks generally refer to two or more computers that are linked together. The Internet networks, through TCP/IP, millions of computers in many different countries, facilitating information exchange: Denton and Menard, *supra* note 70 at 10.

pected to facilitate a greater diversity of expression by freeing speakers from "real-space" reputations or other constraints that might otherwise lead them to self-censor.[73]

Finally, the ideal logical layer would facilitate connectivity through networks of ISPs cooperatively routing the traffic of other ISPs. One 2003 estimate indicated that there were 10 350 ISPs worldwide, of which 760 were located in Canada and 7 000 in the U.S.[74] ISPs act as intermediaries in the process of content transmission and may provide content themselves, host content for others, facilitate access to transmission lines by other ISPs ("backbone service providers") and/or provide users with connections to the Internet ("access providers").[75] Ideally, the availability of a wide variety of ISPs should facilitate a diverse marketplace of ideas. If ISPs do not "screen" the content in respect of which they act merely as a conduit, anyone with a connection to the Internet is free to express him or herself without intermediation or prior restriction. Even if ISPs were to assume responsibility for the content "posted" or "accessed" by their subscribers, it could reasonably be expected that virtually any viewpoint could find a "host" given the sheer number and breadth of ISPs available. Further, given that it is significantly less expensive to become an ISP than to become a publisher in other traditional mass media, content providers who cannot find "hospitable" hosting environments might choose to become ISPs themselves.

Taken together, these elements of the logical layer would ideally facilitate a diverse marketplace of ideas including users with connections around the world, making it more difficult in the U.S. and probably, to some degree, in Canada to justify restrictions on Internet content.[76] Certain privately imposed arrangements within the logical layer, however, may well undermine the diversity frequently *assumed* to exist.

---

[73] While anonymity undoubtedly serves this objective, it also facilitates a lack of accountability and responsibility that may well escalate harmful and damaging expression. Lessig, *supra* note 1 at 177; and Anne Branscomb, "Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspaces" (1995) 104 Yale L.J. 1639 at 1645. Notably, the degree of anonymity available depends, in part on the application in use.

[74] Central Intelligence Agency, The World Factbook—Internet Service Providers (ISPs) (2003), on-line: Central Intelligence Agency http://www.odci.gov/cia/publications/factbook/fields/2152.html (date accessed: 20 August 2003).

[75] *SOCAN*, *supra* note 59 at 433.

[76] Again, however, this is likely only to be true with respect to content otherwise deemed worthy of protection or content determined best addressed through responding content, rather than restriction.

ii. Developments in the Logical Layer

To the extent that TCP/IP permits those at the ends of the network to determine how the network will be used, these protocols facilitate a wide variety of applications, including those that permit identification of users through credit card transactions or through the services of other trusted sources, such as financial institutions. [77] As Lessig points out, development of these applications is in the interest of private business in that they facilitate trustworthy e-commerce by allowing consumers and suppliers to confirm one another's identity.[78] Applications relying on unique IP addresses, combined with other credentialing techniques, may limit diversity by undermining user anonymity and threatening user privacy by making available identifying information about users.[79]

Similarly, recent privately imposed developments relating to ISPs illustrate the departure of the mythologized Internet from the actual. At the inception of the Internet, providers cooperatively routed the traffic of other providers without discrimination or charge in exchange for other providers doing the same. This ideal reflected, at least in part, the relative homogeneity of early Internet uses and users.[80] In that atmosphere, all ISPs and traffic were "equal" in terms of transmission in the Internet marketplace. That relative equality is increasingly rarer. Control over Internet backbone facilities is currently concentrated in the U.S. dominant telecommunications providers that own the largest Tier 1 ISPs that, in turn, control most of the broadband backbone facilities.[81] Tier 1 ISPs no longer necessarily route traffic free of charge and without discrimination for all providers. Rather, those favourable terms are reserved for ISPs able to reciprocate the routing of substantial traffic. Smaller ISPs are charged for transmission

---

77 See: Michael Geist, "Is There a There There? Toward Greater Certainty for Internet Jurisdiction" (2002) 16 Berkeley Technology Law Journal 1 for a detailed review of some of the current technologies.

78 Lessig, *supra* note 1 at 30.

79 Similarly, they may enhance protection for groups frequently targeted by anonymous speech, by forcing speakers to identify themselves with their viewpoint.

80 Robert Frieden, "Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanization" (1998) 3 Va.J.L. & Tech. 8 at paras. 1–2, 11–20.

81 A Tier 1 ISP provides other ISPs with connections to Internet "backbones"—networks spanning large geographic areas. Tier 1 providers include many large telecommunications companies, such as MCI and Sprint in the U.S. and Bell in Canada. See: Robert Frieden, "Revenge of the Bellheads: How the Netheads Lost Control of the Internet" (12 November 2001) at 10-11, online: Social Sciences Research Network http://papers.ssrn. com/sol3/ delivery.cfm/SSRN_ID290121_code011112140.pdf?abstractid=290121 (date accessed: 20 August 2003).

or don't qualify for routing by Tier 1 providers if they are unable to meet certain minimum traffic levels.[82]

To the extent that smaller ISPs might be expected to attract smaller, alternative subscriber bases, these privately negotiated developments undermine the Internet's ability to facilitate the diverse marketplace originally idealized. By advantaging larger, commercial ISPs, some of which have demonstrated a vulnerability to requests for removal of controversial content or have established a market niche based on content monitoring and control,[83] this kind of arrangement threatens the diversity that might otherwise be expected in an ideal marketplace of ideas.

Realities such as these highlight the risk associated with the assuming that the Internet necessarily facilitates the ideal marketplace of ideas—realities that should weigh in the balance in assessing the justifiability of restrictions on Internet content.

2. Efficacy of territorially-based regulation

In *Dagenais*, the SCC noted that technological advances, such as global computer networks, would make it more difficult to justify Canadian-imposed content restrictions under the *Charter*.[84] The Court reasoned that, although Canadian-imposed content restrictions would prohibit dissemination of certain content within Canada, global computer networks would nevertheless give Canadians access to the same content emanating from foreign jurisdictions. In this way, content restrictions imposed in Canada would not achieve their intended salutary effect of eliminating certain content, making their justification under the *Charter* more difficult.[85]

The *Dagenais* decision raised two issues relevant to the logical layer: (i) the technological feasibility of imposing territorially based regulation on Internet content; and (ii) the practical feasibility of enforcing territorially based content

---

82 International Telecommunications Union, Trends in Telecommunication Reform 2000–2001: Interconnection Regulation, 3d ed. (Switzerland: ITU, 2001) at 78–79.

83 The willingness of larger ISPS, such as Yahoo!, AOL, CompuServe and others to engage in private censorship in order to protect their reputations and preserve a sense of "community" among their subscribers is highlighted in further below.

84 *Dagenais v. Canadian Broadcasting Corporation*, [1994] 3 S.C.R. 835 at paras. 89–90. For a detailed discussion of the negative implications of the constitutionality of content restrictions turning on the state of technology at any given time, see: Kerr, *supra* note 2.

85 However, as highlighted below, and explored in detail in Bailey, *supra* note 44, denunciation through public regulation in Canada might also have the effect of encouraging ISPs in other jurisdictions to prevent transmission of certain content into Canada.

regulation against content hosted in a foreign jurisdiction.[86] If the metaphor that the multi-jurisdictional Internet, both technologically and practically, defies territorial regulation is accepted, Canadian-imposed restrictions on Internet content may be more difficult to justify under the *Charter*. However, examination of the logical layer as it began and as it is developing reveal the increasingly tenuous nature of the assumptions inherent in that metaphor.

i. The Logical Layer as it began

It is not difficult to understand how the metaphoric assumption of the borderless Internet evolved, given optimistic predictions about the configuration of the logical layer at the early stages of Internet development.

The simplicity of TCP/IP and the non-identifying nature of IP addresses were expected to facilitate anonymous expression from users connected in jurisdictions around the globe. This particular logical layer configuration created practical hurdles relevant to the *Dagenais* reasoning. If simple protocols prevented the network from "knowing" anything about the content transmitted, except for the IP address at origin and the IP address at destination, it would be difficult to identify users or their geographic location. This could potentially undermine the efficacy of content restrictions even with respect to content emanating from *within* Canada. Further, the multi-jurisdictional nature of connectivity facilitated by TCP/IP allows for content hosted in one jurisdiction to be disseminated to and accessed by connected jurisdictions around the world, with no necessary regard for territorial borders. Finally, by ensuring that end-users, rather than network operators, effectively controlled the uses to be made of the network, TCP/IP facilitated creation of a wide variety of applications, including mirroring applications, which allow content to be copied from a website

---

[86] While both of these potential implications of the *Dagenais* decision will be explored below, the SCC's reasoning ought to be narrowly construed, particularly in relation to the issue of extra-territorial enforceability, for at least three reasons. First, Canadian sovereignty and public policy would be severely undermined if the decision were interpreted to suggest that content restrictions are unconstitutional any time a Canadian order is not enforceable against content disseminated from another jurisdiction around the world. This type of reasoning would deprive Canadians of the ability to make meaningful decisions about the types of content that facilitate or undermine other constitutionally protected rights and values, such as equality and multiculturalism. If that reasoning is accepted, restrictions based on these values would only be enforceable if they were consistent with the values of the least-restrictive nation in the world from which Internet content is disseminated. Second, restrictions on content may continue to serve their intended objectives even if they do not eliminate access to the content in issue by conveying public disapprobation for the content and its harmful effects, which may in turn directly encourage self-censorship. Third, restrictions imposed within Canada should still be effective in eliminating or reducing the distribution of illegal and harmful content from within Canada, even if they were to have little or no effect in eliminating Canadians' access to harmful content emanating from other jurisdictions.

hosted in one jurisdiction to a website in another jurisdiction. As the C.H.R.T. in *Citron* acknowledged, mirroring therefore facilitates circumvention of content regulation imposed in one jurisdiction by moving the content to another, presumably less restrictive, jurisdiction.

The significant number of ISPs around the world, as well as their concentration in the U.S., also challenge the efficacy of Canadian-based content restrictions. Simply put, it is likely to be more difficult to regulate content transmitted through a large number of service and access providers, than that transmitted by a handful of providers.[87] Further, the large number of ISPs, the relatively low cost of becoming a service provider and the early decision of most ISPs not to monitor the content they transmitted, served to enhance the breadth of content—expanding the breadth of the regulatory task. Finally, the geographic dispersion of ISPs around the world meant that content restrictions imposed in one jurisdiction would not necessarily be enforced against ISPs hosting content in another jurisdiction.[88] This dispersion meant that users could avoid enforcement of content restrictions in one jurisdiction by relocating that content to the servers of an ISP in a less restrictive jurisdiction.[89]

i. Developments in the Logical Layer

Developments in the logical layer have addressed the technological feasibility of imposing territorially based content regulation, and have partially answered the practical issue of enforceability. However, enforcement of the content restrictions of one jurisdiction in another jurisdiction continues to pose a challenge—favouring the *de facto* dominance of the law of the least restrictive Internet-connected jurisdiction. In this way, while the configuration of the logical layer continues to present challenges to territorially based regulation, it preserves,

---

87 Effective regulation in the telecommunications and broadcasting sectors historically turned on the presence of one or a few large providers, who submitted to extensive regulation effectively in exchange for protection of their market share from competition.

88 The Yahoo! France case nicely illustrates this point. Although restrictions on hate propaganda are enforceable against ISPs located in France, one U.S. court has ruled they are not enforceable against ISPs facilitating access to content from servers located in the U.S.: *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F.Supp.2d 1181 (N.D.Cal. 2001).

89 Of course, to the extent that the content provider can be identified and is located within the territory of a particular jurisdiction, that jurisdiction can enforce its content regulations against the provider, even if it is prevented from eliminating the content given its location on a server in another jurisdiction. See, for example: Associated Press, "Rare Case Has Norwegian Man Convicted of Racism on the Web", Law.com, on-line: Law.com < http://www.law.com/cgibin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article &cid=ZZZ2CYYEE0D&live=true&cst=1&pc=5&pa=0&s=News&ExpIgnore=true&showsummary=0> (date accessed: 24 April 2002).

and perhaps reinforces, the significance of the geographic location of ISPs and content.

Just as the simplicity of TCP/IP facilitated creation of applications useful in evading territorially based content regulation, it also facilitated creation of applications useful in enforcing it. Geolocational software, developed primarily to permit commercial users to market to certain target audiences, enables increasingly effective (albeit imperfect) identification of user location.[90] These applications make it more difficult for content providers and ISPs to claim it is technologically impossible to comply with the laws in every jurisdiction to which they deliver content—opening up new possibilities for efficacious enforcement. Further, the simplicity of Internet protocols has facilitated use of labeling and filtering technologies in efforts to block prohibited material emanating both from within a jurisdiction and from outside jurisdictions.[91]

Some larger ISPs have departed from their early policies and have begun to monitor and censor not only the content that they may provide, but also the content that they host or to which they provide access. Effectively, these ISPS privately enforce content regulations in the jurisdictions in which they are physically located and in those to which they deliver content. For many ISPs, private monitoring and censorship makes good business sense. Certain service providers, such as AOL[92] and, more recently, EBay[93], have developed market niches based on providing a monitored "community" for users. Others, such as

---

90 Providers of geolocational software claim that it can detect user country location with as much as 95% accuracy, and even narrower pinpoint locations (like city and postal code) with a lower accuracy rate. For a description see: Michael Geist, *supra* note 77, at 52-54. These applications are not foolproof. They can be evaded in a number of ways. See: Anick Jesdanun, "The potential and peril of national Internet boundaries" *The San Francisco Examiner* (7 January 2002), on-line: San Francisco Examiner <http://www.examiner.com /business/default .jsp?story=b.net.0107> (date accessed: 20 August 2003).

91 These types of applications, combined with strict regulation of ISPs, have assisted governments in China and Vietnam to screen out content from "undesireable" locations. See: Greg Walton, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China" (Montreal: International Centre for Human Rights and Democratic Development, 2001), on-line: ICHRDD <http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenMenu.html> (date accessed: 20 August 2003).

92 Letter from AOL Time Warner Inc. to the FCC, "Progress Report on Instant Messaging Interoperability" (July 23, 2001) at 3 [copy available from the author].

93 See: Krysten Crawford, Ebay's Risky Bid" (23 April 2002) Newsbytes, on-line: Law.com <http://www.
law.com/cgibin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c= Article&cid=ZZZ6377QY ZC&live=true&cst =1&pc=0&pa=0>, (date accessed: 23 April 2002), [copy available from the author].

Yahoo! and Google,[94] appear to have been compelled by privately or publicly imposed pressure to engage in more extensive monitoring for "offensive" content, particularly following the September 11th attacks on the U.S.[95]

Thus, the metaphor that the Internet lays beyond territorial boundaries is increasingly being eroded by technological developments facilitated by the simplicity of Internet protocols, as well as by the desire of larger ISPs to maintain solid reputations. In this way, the prospect of effective enforcement of territorially based content regulation has been enhanced. However, the territorial location of ISPs and content continues to present enforcement challenges. Even if inter-jurisdictional enforcement arrangements are agreed upon between nations, the public policy of the territory in which content is physically provided and hosted may prevent legal enforcement of restrictions imposed by other territories.[96] To the extent that the vast majority of content is hosted in the U.S. this territorial reality could allow First Amendment principles to dominate Internet content globally.[97] However, this will not undermine the ability of other jurisdictions, such as Canada, to continue to publicly denounce certain types of harmful expression or to use public regulation to ensure that they do not become safe havens for the disseminators of harmful and illegal content.

---

94 See: Lisa Guernsey, "Yahoo to Try Harder to Rid Postings of Hateful Material" *The New York Times* (3 January 2001), on-line: New York Times <http://www.nytimes.com/2001/01/03/ technology/03YAHO.html> (date accessed: 3 January 2001), [copy available from the author] John Hiler, "Google vs. Church, round 3" Microcontent News, on-line: Microcontent News <http://www.microcontentnews.com/articles/ googleround3.htm> (date accessed: 20 August 2003. Yahoo! has also been criticized for signing a pledge that includes an obligation to restrict and monitor Internet content that the government deems "harmful". See: Jim Hu, "Yahoo yields to Chinese Web laws" (13 August 2002) CNET News, online: CNET< http://news.com.com/2100-1023-949643.html > (date accessed: 20 August 2003).

95 See: Steve Lohr, "I.S.P.'s Curb Terrorist Postings and an Anti-Islamic Backlash" *The New York Times* (17 September 2001), on-line: New York Times <http://www.nytimes.com/2001/09/17/technology /17WEB.html> (date accessed: 17 September 2001), [cop available from the author]. For a detailed analysis of rivate regulatory efforts, see Bailey, *supra* note 44.

96 To the extent that these agreements permit countries to refuse to enforce extra-territorial orders based on public policy, the location of ISPs and content will continue to challenge efficacious inter-jurisdictional enforcement. See for example: *Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters*, 30 October 1999, adopted by the Special Commission to the Hague Conference on Private International Law, Art. 28.1 (f), on-line: Hague Conference <http://www.hcch.net/e/conventions/draft36e.html> (date accessed: 20 August 2003).

97 The sheer number of ISPs and content hosted in the U.S., however, will not necessarily mean that First Amendment principles will dominate. Where the U.S. imposes strict regulations on certain content, as for example in the copyright context, that content is likely to migrate to less restrictive jurisdictions—undermining efficacious enforcement of U.S. laws.

Finally, explicit consideration of the logical layer—in particular the role of ISPs—facilitates examination of other opportunities for regulation within the chain of Internet communications. Whatever the location of the speaker, ISPs located within Canada may become a focal point in efforts to regulate Internet expression, given the intermediary role they play in conveying messages to Canadian users. Moreover, larger ISPs' concern for their corporate reputations may make them ideally suited to assist in limiting the dissemination of harmful and illegal content.

D. The Physical Layer

The physical layer of the Internet relates to the media over which the logical layer operates including fibre optic and coaxial cables conveying Internet content.[98] Analysis of the physical layer assists in exposing the myth that the Internet is an unending, diverse global conversation—a myth that bears directly on the marketplace of ideas concept underlying freedom of expression analysis in both Canada and the U.S.

According to Metcalfe's law, "the value of the network grows as the square of the number of users."[99] Inaccessibility at the physical layer undermines not only the economic value of the Internet, but its expressive value as well, by diminishing the breadth of resources to be exchanged. There can be little doubt that the Internet presents an unprecedented *potential* for a diverse global marketplace of ideas—but the U.S.S.C. was wrong to generalize in *Reno* that the Internet *is* necessarily such a marketplace.[100] Diversity in the marketplace is currently undermined by at least three key elements of the physical layer: (i) the need for a relatively sophisticated telecommunications infrastructure; (ii) distance from servers primarily located in the U.S.; and (iii) factors, such as the cost of gaining access to the Internet, that contribute to a "digital divide" based on race, age, ability, and income levels.

Some regions in the world simply do not have and cannot afford the physical infrastructure necessary to support connectivity.[101] Their residents cannot participate in this marketplace. In other regions, such as Australia and parts of Asia, connectivity is negatively affected by the astronomical cost of physically

---

98 McTaggart, *supra* note 8 at 23.

99 Robert Metcalfe, "The Internet after the Fad", (University of Virginia, 30 May 1996), online: Smithsonian National Museum of American History <http://americanhistory.si.edu/csr/comphist/montic/ metcalfe.htm7> (date accessed: 20 August 2003).

100 In this respect, Internet communication is not unlike traditional telecommunications—neither have achieved truly global penetration.

101 Craig McTaggart, *Governance of the Internet's Infrastructure: Network Policy for the Global Public Network* (LL.M. Thesis, University of Toronto 1999) [unpublished] at 51–52.

connecting to servers and backbones predominantly located in the U.S.[102] In 2001, it was estimated that only 25% of the population in urban India and urban South Africa, had access to the Internet. In urban Russia, an Ipsos-Reid poll showed that 83% of respondents had no Internet access at all.[103] Partially as a result of these physical layer issues,[104] figures released in August, 2003 suggested that almost 30% of on-line users were located in Canada and the U.S., although they represented only about 5% of the world population at that time.[105]

Even within countries with the necessary infrastructure, such as Canada and the U.S., studies reveal a "digital divide" that reflects current social inequalities based on race, ability, and income.[106] As a result, in the U.S., persons

---

[102] International Telecommunications Union, *supra* note 82, at 85-86.

[103] Michael Pastore, "Why the Offline Are Offline" (2001) CyberAtlas, on-line: Cyberatlas <http://asia.internet.com/asia-news/article/0,3916,161_784691,00.html> (date accessed: 20 August 2003).

[104] Inaccessibility in some regions of the world, such as China and Cuba, has also been actively facilitated by government policies designed to block interconnectivity. See: Shanthi Kalathil and Taylor Boas, "The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution" (Washington: Carnegie Endowment for International Peace Working Paper No. 21, Information Revolution and World Politics Project, Global Policy Program, July, 2001), online: Carnegie Endowment for International Peace <http://www.ceip. org/files/Publications/wp21. asp?from =pubauthor> (date accessed: 20 August 2003).

[105] As of August 2003, the U.S. Census Bureau estimated the world population to be 6,312,640,711. As of July 2003, the Bureau estimated the population of Canada to be 32,207,113 and the population of the U.S. to be 290,342,554. U.S. Census Bureau—(2003), online: http://www.census.gov/cgi-bin/ipc/popclockw> and http://www.census.gov/cgi-bin/ipc/idbrunk.pl> (date accessed: 20 August 2003). See also: Global Reach "Global Internet Statistics" (2003), online: http://www.glreach.com/globstats/details.html> date accessed: 20 August 2003).

[106] The U.S. Department of Commerce reported, as of August 2000, a significantly lower access rate for Blacks and Hispanics when compared to whites, and lower access rates for disabled Americans, those with lower income and education levels, and those living in rural areas: U.S. Department of Commerce, "Falling Through the Net: Toward Digital Inclusion" (2000), online: National Telecommunications and Information Administration <http://www.ntia.doc.gov/pdf/fttn00.pdf> (date accessed: 20 August 2003). Similarly, Industry Canada reported, as of October, 2000, significant disparities in Internet access based on income—with significantly higher levels of penetration in households with income above $80,000 than those with income below $40,000. Remote and rural areas are similarly less connected than urban areas: Industry Canada, Retail Council of Canada, "Canadian Consumer Demographics—Canadian Households with Incomes of $80,000 or More—By Technology" (2000), on-line: Industry Canada and the Retail Council of Canada <http://retailinteractive.ca/SSG/ ri00169e.html> (date accessed: 20 August 2003); and Industry Canada, Retail Council of Canada, "Canadian Consumer Demographics—Canadian Households with Incomes of $40,000 or Less—By Technology" (2000), on-line:

of Spanish and African descent, the economically disadvantaged, and those residing in rural areas have been proportionately "less connected" than white, economically advantaged urban dwellers. One North American survey conducted in 30 countries showed that 45% of respondents who did not use the Internet said that they had either no computer (33%) or that they couldn't afford it (12%).[107]

The digital divide is exacerbated further within North America when speed and quality of connection are taken into account.[108] While broadband access facilitates use of a broader range of Internet applications, it is frequently not available or affordable in remote regions. As a result, although Canada has impressive Internet penetration rates when compared with the rest of the world,[109] Inuit and First Nations people residing in northern regions have been disproportionately affected by the physical inaccessibility of this type of Internet connection.[110] Although clearly not as serious as having no access, the inaccessibility of broadband services is likely to become increasingly problematic as new Internet technologies requiring high-speed connections are developed.[111]

Whether these physical layer issues would ultimately affect the outcome of constitutional analysis of restrictions on expression in Canada or the U.S. will depend, in part, on the nature of the expression in issue. As set out above, Canadian and U.S. courts have determined that certain types of expression merit little or no constitutional protection. In these cases, the lack of diversity generated by certain elements of the physical layer is unlikely to affect the outcome of the constitutional analysis. However, in other cases, where the assumption of global diversity and participation might have tipped the constitutional balance against restrictions, recognition of the physical limitations on diversity may affect that balance.[112] In any event, these elements of the physical layer illustrate

---

Industry Canada and the Retail Council of Canada <http://retailinteractive.ca/SSG/ri00167e.html> (date accessed: 20 August 2003).

107 Pastore, *supra* note 103.

108 U.S. Department of Commerce, *supra* note 106.

109 Craig McTaggart, "IP Telephony and the Internet: Canada Case Study" (3d World Telecommunications Policy Forum on IP Telephony, Geneva 29 March 2000) at 21.

110 Canada, *Report of the National Broadband Task Force: The New National Dream: Networking for Broadband Access* (Ottawa: Industry Canada, 2001) (Chair: David Johnston), online: Industry Canada < http://broadband.gc.ca/broadband-document/broadband.pdf> (date accessed: 20 August 2003).

111 Charles Platt,"The Future Will be Fast But Not Free" (May 2001) Wired, online: Wired, < http://www. wired.com/wired/archive/9.05/broadband.html> (date accessed: 20 August 2003).

112 These are likely to be the cases where the harm associated with particular expression is thought to be best addressed through responding expression, rather than through censor-

an important methodological point: generalizations about the global and diverse nature of the Internet must be approached with caution. To proceed otherwise is to risk basing important constitutional decisions on a myth that conflates what the Internet *is* with what it has been idealized to be.

V. CONCLUSION

The layered methodology contributes to the constitutional analysis of content regulation by encouraging a move away from generalizations about the Internet as a whole, toward examination of some of the component elements that contribute to determining what the Internet is and can be. No single layer can be expected to be determinative in terms of constitutional analysis of Internet content regulations, either in Canada or in the U.S. Rather, elements within each of the content, applications, logical and physical layers will contribute to a more robust analysis of the empirical and normative questions as to whether Internet content *can* and *should* be regulated.

The content layer relates most closely to the question of whether Internet expression *should* be regulated. Certain types of content, regardless of the medium of communication, will not be considered to merit constitutional protection either in the U.S. or in Canada, although the courts in the two countries do not necessarily agree as to which content falls into this category.[113] Courts relying on the "marketplace" model may be tempted to conclude that the virtually unprecedented scope of content available on the internet makes government regulation even more difficult to justify. However, for reasons most evident at the logical and physical layers, courts should be cautious about assuming that restrictions on Internet content necessarily constitute wide-ranging restrictions on global expression.

Examination of the applications layer illuminates the myth that the Internet can be categorized as public or private in nature. Recognition of the myth is essential in thinking about whether content available on the Internet *should* be regulated. Given constitutional privacy commitments in both Canada and the U.S., it is essential to recognize that the "Internet" cannot be monolithically characterized as private or public in nature. Rather, different applications may

---

ship. This approach is regularly reflected in U.S. constitutional decision-making. See: Steven Gey, "Fear of Freedom: The New Speech Regulation in Cyberspace" (1999) 8 Tex. J. Women & l. 183; Laurence Tribe, *American Constitutional Law* (2d) (Mineola, New York: The Foundation Press, 1988) at 793–794.

[113] Further, the types of content meriting less protection may change, having regard to the nature of certain forms of Internet communication. Where, for example, an Internet application provides an ability to respond promptly and that ability would meaningfully address the potential harm arising from the content in issue, it may be that restrictions on that content will be more difficult to justify in the Internet context than in relation to other media.

be more privacy-invasive than others and may create differing expectations of privacy. In this way, applications, the type of content and the particular use made of an application in a given circumstance will be relevant when assessing whether content *should* be restricted in any particular case.

Examination of the logical layer facilitates recognition of the twin myths that the Internet necessarily reflects a diverse, global marketplace of ideas and that it necessarily defies territorial regulation. Illumination of these myths is important in determining both whether Internet content *can* and *should* be regulated. IP addressing, simple accessible protocols, and the large number and dispersion of ISPs could facilitate a diverse and anonymous marketplace of ideas free of intermediary interference. However, at the same time, protocol simplicity and IP addressing make possible applications facilitating user identification that, in turn, undermine anonymity. Similarly, private peering arrangements between ISPs, combined with private censorship restrict diversity with little public accountability. As a result, courts need not assume that Internet content *should* not be regulated because restrictions necessarily constitute censorship of an ideal marketplace of ideas. Further, protocol simplicity facilitating networking of users and ISPs in jurisdictions around the world challenges efficacious territorial regulation—a matter that may be of significance in Canadian constitutional analysis if the reasoning in *Dagenais* is interpreted too broadly. However, this simplicity has also facilitated geolocational technologies, which when combined with ISP willingness to restrict harmful and illegal content, makes more effective territorial regulation increasingly possible. As such, Canadian courts should not assume that effective territorial regulation of Internet content *cannot* technically be accomplished

Examination of the physical layer also highlights the mythical nature of the assumption that the Internet facilitates a diverse, global marketplace of ideas. Physical layer elements reveal the degree to which the lack of infrastructure, geographic distance from the U.S. and factors restricting user access undermine the *actual* diversity within the Internet marketplace. Therefore, when courts ask whether we *should* regulate Internet content, examination of the physical layer illustrates that they need not assume that restrictions on Internet content are tantamount to restrictions on an ideal global marketplace of ideas.

Use of a layered methodology will not necessarily change the outcome of constitutional analyses of restrictions on Internet expression. However, it should facilitate a more explicit examination of the elements that affect what Internet communication *is*, *was* and *can be*—elements that may be material to maintaining existing public and constitutional values.