

# **Regulation of Internet Content in Canada and Implications for the Charter**

**By Corey D. Steinberg**

**Steinberg Morton Hope & Israel LLP  
April 30, 1999**

## **(I) Introduction**

The Internet is the most dynamic and diverse medium to be developed by modern society. This new 'information superhighway' is imbued with the ability to provide a user with valuable information pertaining to a plethora of subjects and issues. The Internet also has the capacity to provide users with a variety of forms of entertainment, ranging from music to pornography. It is natural for governments to wish to regulate the content of the Internet available to those in their jurisdiction.

Regulation of Internet content, however, is a concept replete with problems for a government such as that of Canada. Enacting legislation that would be both effective and constitutional would be difficult. Further, if such legislation could be enacted, it is questionable whether or not it would be technologically possible to enforce such a law in a constitutional manner.

## **(II) The Communications Decency Act of 1996 and *Reno v. ACLU***

The enactment of the *Communications Decency Act*<sup>i</sup> in the United States of America represented an attempt by the American authorities to regulate Internet content based on a community standard of morality and the vague criteria of 'indecent' and 'patently offensive.' This piece of legislation was struck down as contrary to the First Amendment of the American Constitution. This was a result of the landmark decision by the United States Supreme Court in the case of *Reno v. ACLU*.<sup>ii</sup>

The judgment in *Reno*<sup>iii</sup> held that this legislation was an impermissible restriction on the First Amendment rights of adults. The First Amendment is the provision in the American Constitution, which protects the right to free speech.

Justice John Paul Stevens wrote the judgment for the majority. The ruling held that speech on the Internet must be afforded the highest level of constitutional protection. He likened the new medium to books and newspapers, which receive similar protection.

The medium was found to be less pervasive than television. The court found this to be so due to the active search required of Internet users to find indecent material. The court cited *Sable Communications of California, Inc. v. F.C.C.*,<sup>iv</sup> wherein the court invalidated a ban on 'dial-a-porn', as the most applicable case to that of *Reno*<sup>v</sup>. This was found because the active search necessary to find pornography on the Internet is analogous to that implemented when accessing telephone pornography.

Nathan M. Semmel of the *New York Law School Journal of Human Rights* explains the *ratio decidendi* in *Reno*<sup>vi</sup>:

"Despite finding the protection of children a compelling governmental purpose, Justice Stevens, applying the rationale of *Sable*, found the defense provided for in the Act not to be sufficiently tailored so that adult access to constitutionally protected material was least restricted. In most cases, individuals would truly have been left with only one option - censorship. Because the government failed to proffer any less restrictive alternative than those offered in Section 223(e), the Communications Decency Act of 1996 could not be sustained."<sup>vii</sup>

Justice Stevens' ruling also addressed the argument that 'obscene material is limiting the rate of growth of the Internet by turning users away.' It was contended that such an obstacle to the Internet's growth is interfering with the free exchange of ideas. Essentially, it was argued that the vast array of obscene material on the Internet was causing many would-be users to forego usage of the new medium in order to avoid such offensive content.

This argument proved unfounded when confronted with evidence of the exponential growth rate of the Internet. On the contrary, evidence would indicate that any governmental regulation would be more likely to interfere with the free exchange of

ideas than to encourage such interaction. As the matter was not definitively proven either way, the court held that society's interest in encouraging free expression must outweigh any "theoretical but unproven" benefits that might be derived from censoring this medium.<sup>viii</sup>

Stevens J. explains on behalf of the majority:

"As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it."<sup>ix</sup>

### **(III) Would the *Communications Decency Act*<sup>x</sup> Be Constitutional in Canada?**

#### **(A) The *Oakes*<sup>xi</sup> Test and Section One of the Charter<sup>xii</sup>**

Traditionally, Canada has looked to other jurisdictions as a guide to resolving disputes that are unlike any litigated in a Canadian court. Historically, Canada has been influenced by English jurisprudence; however, American case law is becoming increasingly influential. This has been a result of two factors. One reason is that the U.S.A. is geographically and culturally similar to Canada, and the second is that the Americans tend to litigate cutting-edge matters more readily than those in other jurisdictions.

The Canadian Legislature has yet to enact a law regulating content on the Internet. For this reason, Canadian courts are yet to examine legislation comparable to the CDA.<sup>xiii</sup> It is possible, however, to anticipate how such a law would fare according to the *Canadian Charter of Rights and Freedoms*<sup>xiv</sup> by examining the American example compared with existing Canadian case law.

In the judgment in *Reno*,<sup>xv</sup> Stevens J. said, "We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of

free speech."<sup>xvi</sup> In Canada, this statement is echoed, at least in spirit, in the 1986 Supreme Court of Canada case, *R. v. Oakes*.<sup>xvii</sup> In the judgment of that case the test for the constitutionality of legislation that infringes the *Canadian Charter*<sup>xviii</sup> was outlined. The objective of this test is to determine if a limit on a *Charter* right is valid and thereby 'saved' under Section 1 of the *Charter*.<sup>xix</sup>

Section 1 states:

"The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."<sup>xx</sup>

The test to determine if a limit on a *Charter*<sup>xxi</sup> right is justified under Section 1 is outlined in the *Oakes*<sup>xxii</sup> judgment as follows:

"First, the objective to be served by the measures limiting a Charter right must be sufficiently important to warrant overriding a constitutionally protected right or freedom. The standard must be high ... At a minimum, an objective must relate to societal concerns which are pressing and substantial ... Second, the party invoking s. 1 must show the means to be reasonable and demonstrably justified. ... (T)he measures must be fair and not arbitrary, carefully designed to achieve the objective in question and rationally connected to that objective. In addition, **the means should impair the right in question as little as possible.** (*editor's emphasis*) Lastly, there must be a proportionality between the effects of the limiting measure and the objective - the more severe the deleterious effects of a measure, the more important the objective must be."<sup>xxiii</sup>

If a piece of legislation fails on any aspect of the *Oakes* test, it is not saved under Section 1 of the *Charter*. For this reason, for our purposes, although this law would likely fail other aspects of the test as well, it is sufficient to examine a single provision of the *Oakes*<sup>xxiv</sup> test. This provision is the factor comprising part of the second criterion that "the means should impair the right in question as little as possible."<sup>xxv</sup>

This provision is comparable to the statement of Justice Stevens in *Reno* that "the CDA lacks the precision that the First Amendment requires when a statute regulates the content of free speech."<sup>xxvi</sup> This provision, in both the Canadian ruling and (what I have

argued is) its American counterpart, requires that fundamental rights and freedoms, if they absolutely must be limited, must be restricted minimally; i.e. only within the *de minimis* range.

**(B) Would the *Communications Decency Act*<sup>xxvii</sup> Satisfy the *Oakes* Test?**

**(i) *R. v. Zündel*<sup>xxviii</sup>**

The CDA<sup>xxix</sup> did not survive a constitutional challenge in the United States. It failed on the basis that it lacked the "precision" necessary to be a limit on a fundamental right. If it lacked this precision in the United States, it stands to reason that this type of legislation would arguably also be an unsupportable limit on a Canadian *Charter*<sup>xxx</sup> right.

An examination of the relevant case law also leads to the above conclusion. The case of *R. v. Zündel*<sup>xxxi</sup> is an example of the Supreme Court of Canada examining a law which seeks to limit the Canadian right to freedom of expression.

Ernst Zündel was a schoolteacher disseminating literature that denied the existence of the Holocaust. He was charged under Section 181 of the *Criminal Code of Canada*.

That section states:

"Every one who wilfully publishes a statement, tale or news that he knows is false and that causes or is likely to cause injury or mischief to a public interest is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years."<sup>xxxii</sup>

The court found that this statute was contrary to Section 2(b) of the *Charter*,<sup>xxxiii</sup> which is the provision protecting freedom of expression. This legislation failed the *Oakes*<sup>xxxiv</sup> test at every step. Specifically relevant to our examination of the CDA,<sup>xxxv</sup> the court found that Section 181 of the *Criminal Code* was overbroad due to vagueness.

Provisions such as 'knowing' that information is 'false' or 'likely to cause injury or mischief' are not sufficiently narrowly defined to constitute an acceptable limit on a *Charter*<sup>xxxvi</sup> right.

Writing for the majority, McLachlin J. wrote:

"Section 181 catches not only deliberate falsehoods which promote hatred, but sanctions all false assertions which the prosecutor believes 'likely to cause injury or mischief to a public interest,' regardless of whether they promote the values underlying s. 2(b)."<sup>xxxvii</sup>

The court's concern was not for hate-mongers such as Zündel. The bench feared for those who might wish to communicate legitimate information or grievances that could benefit society if publicized. These individuals could be silenced out of a concern that they be deemed to have 'known' that their 'assertions' were 'false' (if such proves subsequently to be the case) and that they were 'likely to cause injury or mischief to a public interest.'

McLachlin J. delineates this danger:

"Section 181 can be used to inhibit statements which society considers should be inhibited, like those which denigrate vulnerable groups. Its danger, however, lies in the fact that by its broad reach it criminalizes a vast penumbra of other statements merely because they might be thought to constitute a mischief to some public interest ... The danger is magnified because the prohibition affects not only those caught and prosecuted, but those who may refrain from saying what they would like to because of the fear that they will be caught. Thus worthy minority groups or individuals may be inhibited from saying what they desire to say for fear that they might be prosecuted."<sup>xxxviii</sup>

For example, vegetarian organizations in beef producing regions such as Alberta could be prosecuted. They could be charged on the basis that it is 'likely' that their public assertions would cause 'injury or mischief to a public interest,' specifically the local beef industry. A further example would be scientists with evidence to endorse the legitimacy of such politically charged theories as evolution. These individuals could be prosecuted for publishing such experimental results as it is 'likely' that these assertions would also

cause 'injury or mischief to a public interest' by offending the sensitivities of society's Religious Right. An individual involved in a matter similar to either of these two examples could choose to remain silent out of fear of prosecution, in case her information proves to be false and she be deemed to have known this.

McLachlin J. extols this very concern:

"Should an activist be prevented from saying "the rainforest of British Columbia is being destroyed" because she fears criminal prosecution for spreading "false news" in the event that scientists conclude and a jury accepts that the statement is false and that it is likely to cause mischief to the British Columbia forest industry? Should a concerned citizen fear prosecution for stating in the course of political debate that a nuclear power plant in her neighbourhood "is destroying the health of the children living nearby" for fear that scientific studies will later show that the injury was minimal? Should a medical professional be precluded from describing an outbreak of meningitis as an epidemic for fear that a government or private organization will conclude and a jury accept that his statement is a deliberate assertion of a false fact? Should a member of an ethnic minority whose brethren are being persecuted abroad be prevented from stating that the government has systematically ignored his compatriots' plight? These examples suggest there is merit in the submission of the Canadian Civil Liberties Association that the overbreadth of s. 181 poses greater danger to minority interest groups worthy of popular support than it offers protection."<sup>xxxix</sup>

The CDA<sup>xi</sup> is comparable to Section 181 of the *Criminal Code of Canada*<sup>xli</sup> in many ways. Particularly the CDA<sup>xlii</sup> has the self-proclaimed object of preventing 'indecent' and 'patently offensive' content from reaching the RAM<sup>xliii</sup> of Americans. Section 181 has the analogous object of preventing 'false' information that is 'likely to cause injury or mischief to a public interest' from being publicized in any manner in Canada. This object of Section 181 was held by the Supreme Court to be an overbroad limit on the right of freedom of expression. It is reasonable, therefore, to suppose that the comparably vague standards by which the CDA<sup>xliv</sup> seeks to limit freedom of expression would also be deemed insufficiently tailored to amount to a justifiable limit on a *Charter* right under supreme<sup>xlv</sup> Canadian law.

(ii) *R. v. Butler*<sup>xlvi</sup>

The criterion of 'indecent,' as it appears in the CDA,<sup>xlvii</sup> is defined by American courts according to a 'community standards test.'<sup>xlviii</sup> This is a test to determine what will offend the standards of decency in a given community. Content that will offend is deemed outside the 'community standards.'

This is a dangerous criterion upon which to base legislation as it will invariably be the most hypersensitive members of any community who will attempt to define the standard to meet their own threshold. Such a system will tend to limit the whole community to a 'lowest common denominator' based on the sensitivities of those most easily offended. This standard holds serious potential ramifications for a community as wide and diverse as that of the Internet.

Stevens J. explains in *Reno*:<sup>xlix</sup>

"The "community standards" criterion as applied to the Internet means that any communication available to a nation-wide audience will be judged by the standards of the community most likely to be offended by the message."<sup>l</sup>

In Canada, the 'community standards test' has been refined. The Canadian version, however, is neither more definite nor more suited to cyberspace than its American counterpart. The Supreme Court of Canada outlined this standard in the case of *R. v. Butler*.<sup>li</sup> Instead of the American standard defined by what is 'offensive' to the community, the Canadian test proscribes content that is 'intolerable' to a community for others to consume.

The court found in *Butler*:

"The cases all emphasize that it is a standard of *tolerance*, not taste, that is relevant. What matters is not what Canadians think is right for themselves to see. What matters is what Canadians would not abide

other Canadians seeing because it would be beyond the contemporary Canadian standard of tolerance to allow them to see it."<sup>lii</sup>

This Canadian test for obscenity is not sufficiently narrowly defined to apply to the Internet. Such a standard would result in overbroad legislation. A law based on this standard would censor content available to *every* Canadian in cyberspace according to that which is tolerable within the 'contemporary Canadian standard' to be viewed by *anyone* surfing the Net. This would amount to censoring Internet content to a level appropriate for the youngest and most innocent members of society.

Those that comprise the community of the Internet are a diverse group. It would be overly restrictive to limit every Net surfer's access to content tolerable for the consumption of the youngest of children represented in cyberspace. Such a restriction could hardly satisfy the spirit of the *Oakes*<sup>liii</sup> test, which restricts any limitation on a *Charter*<sup>liv</sup> right to that within the *de minimis* range.

**(C) Legislation Comparable to The *Communications Decency Act*<sup>lv</sup> Would be Overbroad for Canada: But is it Technologically Possible to Sufficiently Narrowly Define Such a Law?**

An examination, thus, of Canadian case law as it applies to the CDA<sup>lvi</sup> indicates that, if enacted in Canada, it would not be an acceptable limit on the *Charter*<sup>lvii</sup> right protecting freedom of expression. Legislation based on criteria such as 'indecent' or a 'community standard' would not satisfy Section 1 of the *Charter*<sup>lviii</sup> when subjected to the *Oakes*<sup>lix</sup> test.

Questions pertaining to the specificity of such limitations on a *Charter*<sup>lx</sup> right, however, may be found superfluous upon an examination of the technology itself. It may prove moot to discuss the breadth of such laws considering the options that would be

available to practically implement such legislation. It is arguable that the means currently available to regulate Internet content may also be overly restrictive when subjected to the *Oakes*<sup>lxi</sup> test.

#### **(IV) Filtration Software**

##### **(A) Introduction to the Technology Available to Governments Who Would Seek to Censor Internet Content**

One factor that relegates the regulation of Internet content to the realm of the unconstitutional is also a problem inherent in the technology itself. The problem is analogous to that ensuing from the imprecision inherent in the CDA<sup>lxii</sup> as 'overbroad legislation'. This problem was indirectly acknowledged by the U.S. Supreme Court in *Reno*,<sup>lxiii</sup> concurring with a finding by a specially convened three-judge court, which had heard the case previously.<sup>lxiv</sup>

The *Communications Decency Act*<sup>lxv</sup> uses terms such as 'indecent' and 'patently offensive' as criteria for restriction to access to content on the Internet. The court recognized that such criteria, "cover large amounts of nonpornographic (*sic*) material with serious educational or other value."<sup>lxvi</sup> Justice Stevens maintained that the court found "no textual support for the Government's submission that material having scientific, educational, or other redeeming social value will necessarily fall outside the CDA's "patently offensive" and "indecent" prohibitions."<sup>lxvii</sup>

The same concerns arise when examining the technological remedies available to those that would seek to regulate cyberspace. Currently, the only viable method of blocking 'indecent' material from entering the computers of North America would undoubtedly restrict the free flow of scientific and educational information as well.

Internet users, or 'Netizens,' know the method in question as *filtration software* and it comes in many forms and packages.<sup>lxviii</sup> At a more general level, however, there are essentially two different types of filtration software available, which can be divided into *database systems of filters* and *embedded systems*.

## **(B) Database Filtration Systems**

### **(i) How a Database Filtration Program Works**

Database systems of filters associate a particular rating with the content comprising a particular site on the Internet. When a user requests a particular piece of information, her system contacts the database. The database then sends back the corresponding rating. Sites rated at a level deemed 'inappropriate' by the filtration program are blocked and will be unavailable to the user.

The U.S. Supreme Court indirectly recognized one of the most alarming failings of such programs. Like the CDA,<sup>lxix</sup> such mechanical means of regulating Internet content have a tendency to be overbroad. Rather than merely filtering content that could arguably be deemed obscene, such systems also have a tendency to block information relating to matters of genuine and pressing social concern.

Lawrence Lessig expresses his apprehension:

"Horror stories abound - sites opened to criticize blocking software (are) themselves included in the blocked list, sites opened to discuss AIDS, or gay rights, excluded because of "mistaken" associations with indecency, vegetarian pages excluded because of associations with animal rights movements. Controversial sites are easily excluded, yet no one says who gets cut."<sup>lxx</sup>

Apart from concerns of overbreadth, this type of filtration program has serious practical limitations. Even if such systems could be honed to only filter out 'indecent' content such systems are limited by being grounded in a database of watchwords.<sup>lxxi</sup>

Such a system is static. The Internet, on the other hand, is the most dynamic medium society has yet developed. The idea of applying a static system to regulate a dynamic medium is inherently flawed and doomed to failure over the long term.

**(ii) Why a Database Filtration System is Inappropriate for the Net**

The content of the Internet has increased and evolved over the years and this evolution is bound to continue. A regulation schema that is not suited to change will eventually fall short. It is not possible for producers of database filtration software to anticipate any and all means of posting 'indecent' material. "(S)ophisticated hackers are able to hide obscene images and text within other seemingly innocent postings, and decoding techniques can be rapidly circulated among members of the computer underground."<sup>lxxii</sup>

Even if it were possible for database filtration programs to decode such 'encrypted'<sup>lxxiii</sup> messages, it would be impossible to implement such a system of watchwords in any practical way. These filters rely on dictionaries of words and phrases in order to block particular material. For this reason it would be impossible to adapt such a system such that it would be neither over-inclusive nor under-inclusive.

Carlin Meyer expresses his concern:

"No matter how inclusive such a dictionary is, it cannot possibly embrace the enormous variety of words used to create obscene stories or to describe obscene images."<sup>lxxiv</sup>

Database filtration systems would not be likely to block, for instance, a descriptor such as "Woman! Horse! Hot!"<sup>lxxv</sup> Such a caption would be an obvious description of a bestiality site, to a human censor, but would pass entirely undetected by a database filtration program.

The inclusion of watchwords in the database, such as those in the above example, would not be feasible. It would trigger the problem already discussed of filtering 'decent' content from a user's computer along with 'indecent' content. If these words were included the absurd result would be a prevention of the user from accessing websites pertaining to women's issues, farm animal care, and even sites posting weather and temperature forecasts.

**(iii) How Can a User Ever Know What is Being Filtered?**

A further concern that arises from database filtering systems is the great degree of ignorance under which a user is forced to operate when utilizing such a program. A user has no means of knowing what is being blocked from her computer. Moreover, even if she could figure out what was being blocked, she would have no means of finding out why any particular site is blocked. "(O)ne can't know what sites are on these lists, and there's no simple way to verify that sites are not included for the wrong reasons."<sup>lxxvi</sup>

The situation is analogous to a list of banned books that have been burned so as not to reach the public. In the case of a book burning, these events were generally held in public so that people were aware of the titles from which they were being 'protected'. In this case, however, it is not even possible to see the list of 'burned books' (or filtered websites) in order to know what sort of material is being censored.

This problem is a result of the computer industry's traditionally religious adherence to the protection of intellectual property. Creators of database filtration programs consider the information constituting these databases to be proprietary material in the form of trade secrets. As such, the programmers of such systems closely guard

these lists. Further, as trade secrets, the contents of such lists are subject only to the judgment of the programmers involved.

**(iv) Database Filtration Systems Would Render Any Legislation Unconstitutional**

Database filtration systems are simply inappropriate as a tool to regulate content on the Internet. They are both over-inclusive and under-inclusive. They are designed autocratically and are subject only to the standards of their creators. Such a system would be wholly inappropriate, as a means for the government to implement any sort of legislation. It, undoubtedly, would be an overbroad limit on freedom of expression.

Even if a law could be enacted which regulates Internet content for Canadians and is deemed an acceptable limit on a *Charter*<sup>lxxvii</sup> right, implementation of such a law by a database filtration system would be an overbroad limit. Such filtration programs themselves are replete with the same limitations that would render legislation such as the CDA<sup>lxxviii</sup> unconstitutional in Canada. It is obvious, therefore, that if the government were to regulate access to Internet content, a database filtration system would not be a workable means of implementing such regulation.

**(C) Embedded Filtration Systems: Could PICS Be the Solution for Governments Who Seek to Regulate Internet Content?**

**(i) How an Embedded Filtration System Works**

Embedded filtration systems are tags that are 'attached' to websites themselves. These are labels to be used by rating systems, embedded within Internet content itself that rate a site based on a number of specified criteria. Such a system is far less haphazard and vague than a database filtration system as it necessarily involves the cooperation of the website producer in order to be implemented pursuant to that site.

Cooperation is necessary, as it is the creator of the site that must add a line of encoded information to the HTML coding of the page. This information describes the site in terms understandable to an external rating system. This information acts as a tag that can be read by commercially available software. The software program grades the site based on the tag. According to this grading, the site is either filtered out, or allowed to pass on to the user's computer screen.

**(ii) PICS: The Most Likely Candidate for an Embedded System**

Currently, the most potentially viable embedded system is called *The Platform for Internet Content Selection* (PICS). Paul Resnik of AT&T Research and James Miller of MIT developed this system as a means of regulating Internet content according to different standards as imposed by different communities.<sup>lxxxix</sup>

R. Polk Wagner gives a concise explanation of how PICS works:

"PICS itself specifies little more than the syntax and protocols used to label content and transmit the labels; it does not itself specify a ratings system. The creators of PICS intend to enable other groups (or even individuals) to develop their own rating schemes, using PICS as the underlying standard to ensure interoperability. Thus, for example, any web browser that is PICS-enabled would be able to use any of the PICS-compatible ratings systems. A market might then develop for such ratings systems, allowing a diversity of ratings systems as well as placing the choices regarding rating and viewing content in the hands of the producers and users, respectively."<sup>lxxxix</sup>

Resnik and Miller believe that such a system will solve many of the problems arising from diversity issues that necessarily come into play whenever discussing the Internet and the regulation thereof. Resnik and Miller recognize that governments around the world are considering regulation of this medium. Problems abound, however, stemming from the fact that all national and cultural contexts are not homogeneous.

Children differ worldwide. Furthermore, contexts of Internet use and values differ as national and cultural borders are crossed. For this reason, universal blanket

restrictions would not be feasible. A diverse market of rating systems,<sup>lxxxii</sup> however, could address this problem of national and cultural diversity. Raw data in the form of PICS tags could be a viable resource from which such rating systems may draw information and regulate content accordingly based on a nationally or culturally specific rating and filtration program.<sup>lxxxiii</sup>

**(iii) Could Embedded Filtration Systems Solve the Constitutional Problems That Would Face Canadian Legislators Attempting to Regulate Internet Content?**

Such an embedded filtration system could be a potential solution for the Canadian government if it were seeking to regulate Internet content. Assuming that legislation could be written that is specific enough to pass Canadian *Charter* muster, perhaps an embedded filtration system could be used to implement such legislation in a constitutional way.

Such a system avoids many of the problems inherent in a database filtration system, which arise as a result of websites being judged and filtered by third parties. An embedded system allows a site producer to rate her own site. Further, the user may choose a particular rating system that will or will not filter out sites with such a rating.

R. Polk Wagner explains the advantages of such a system:

"Conceptually, an embedded ratings system seeks to solve the major problems of the database systems by shifting the responsibility of rating content to the producer and transmitting the rating with the content itself. Thus, an embedded system wholly avoids the volume problem fundamental to the database systems. Further, by "labeling" or "tagging" each page or other element of content, the embedded system is neither under- nor overbroad. And because producers rate their own content as they create it, the rating system is comprehensive, and the third-party effects ... are not present."<sup>lxxxiii</sup>

**(iv) Enforceability of an Embedded Filtration System**

In order for a system like PICS to work the site producers must rate the content of their sites honestly and according to universal criteria. Enforcement of such a system would be difficult but not impossible.

As it is foreseeable that some unscrupulous site producers will intentionally rate their sites incorrectly, in order to reach an unsuspecting audience, enforcement of a system such as PICS must come, primarily, from the users of particular programs. As offensive pages pass by the program undetected, users of this program must accept the responsibility of informing the program manufacturer. The site may then be reevaluated and rated accordingly.<sup>lxxxiv</sup>

The question arises, however, as to what should be done if site producers choose to ignore the rating system altogether. In cases of sites with no rating at all, the program designated to filter content will be unable to distinguish acceptable content from unacceptable content. How could an embedded filtration system accommodate such sites? The answer to this question also lies with the users of such programs.

These programs could be equipped with a changeable default setting allowing the user to decide for herself whether to accept unrated sites onto her monitor or not. Users could choose to be shown unrated sites and then simply close them, or to have such sites excluded outright. If a system like PICS gains enough popularity<sup>lxxxv</sup> and users tend to choose the option of excluding unrated sites such market dynamics will be self-regulating. Producers will find no choice but to rate their sites in order to reach a significant audience.

Wagner comments:

"For example, version 4.0 of Microsoft's Internet Explorer allows the user to check a box to choose whether unrated pages can be seen. The implied threat of opt-out by users will, in theory at least, encourage

many commercial web sites to rate their pages according to the most popular rating services. One can imagine that if PICS gains a powerful following among the public, the pressure on producers to label content will only increase."<sup>lxxxvi</sup>

#### **(iv) Upstream vs. Downstream Embedded Filtration Systems**

A system like PICS is useable at any juncture in the flow of data from the Internet. "The flow of content through the Internet is analogous to a stream. The content service provider is at the head of the stream, and the Internet users are downstream."<sup>lxxxvii</sup>

Resnik and Miller designed the system with the expectation that filtering will occur "downstream"<sup>lxxxviii</sup> at the level of the user, but such a system could be implemented at any node between the site operator and the user. This includes but is not exclusive to the Internet service provider as well as the regional network access point.

The fact that such filtration can occur at any juncture endows it with the potential application as a tool of government censors. The Canadian government would have the option of using such a system in order to enforce a law regulating Internet content, if such a law could be written in a manner that would pass a *Charter* challenge.

#### **(v) PICS Upstream Would Not Pass a *Charter* Challenge**

Suppose an embedded system such as PICS were used "upstream" at the behest of a governing body, rather than "downstream"<sup>lxxxix</sup> at the user level. "The Federal, state, (provincial in Canada <ed.>) or local government could simply filter Internet content itself or force the filtration of all Internet content by third parties, such as ISPs or backbone carriers."<sup>xc</sup> Such a limit on the flow of content could not pass a Section 1 *Oakes*<sup>xc</sup> test as a limit on freedom of expression within the *de minimis* range. The main reason that such an imposition of censorship would not be saved under a Section 1 analysis is that it would be applied indiscriminately regardless of a user's age.

Putting aside the issue of what content children should or should not have a constitutionally protected right to view,<sup>xcii</sup> there is no question that adults often have a legal right to consume content from which children are legally prohibited. For instance Canadian children are prohibited from seeing "Restricted" movies, which adults have a right to see. Children are also prohibited from buying magazines deemed pornographic that adults may purchase at any convenience store.

An application of PICS "upstream"<sup>xciii</sup> would result in the absurd situation of restricting adults' access to Internet content on the basis of a rating acceptable for a child to view. All Internet users would be treated alike. This would be the only means of 'protecting' children from Internet content that would only be acceptable for an adult's consumption.

Such an implementation of legislation regulating Internet content would be overbroad due to vagueness. This is analogous to the ruling that the CDA<sup>xciv</sup> is unconstitutional in *Reno*.<sup>xcv</sup> This is also analogous to the argument above that the CDA<sup>xcvi</sup> would be contrary to case law and the *Charter*<sup>xcvii</sup> in Canada. If legislation were enacted to regulate Internet content such a law could not be constitutionally enforced by filtration "upstream,"<sup>xcviii</sup> even by an embedded filtration system.

## **(V) The Laissez-Fair Approach**

### **(A) Regulation of Internet Content in Canada Could Not Meet a Charter Challenge**

An examination of the current potential for regulating Internet content reveals a daunting task. The American CDA<sup>xcix</sup> was proven unconstitutional in *Reno*.<sup>c</sup> It was found to be vague and an overbroad restriction on free speech. Upon examining this

legislation against the Canadian legal system, it appears certain that such a law also would not survive a *Charter*<sup>ci</sup> challenge in a Canadian court.

Even if such legislation could be written such that it were constitutional, it appears that the technology available to regulate Internet content is not precise enough to survive a *Charter*<sup>cii</sup> challenge if implemented "upstream"<sup>ciii</sup> by the Canadian government. A *database filtration system* would be both over-inclusive and under-inclusive. An *embedded filtration system*, such as PICS would be more adaptable and precise, but if imposed "upstream"<sup>civ</sup> would still result in 'protecting' adults from the same content from which the government seeks to 'protect' children. If implemented "upstream,"<sup>cv</sup> either type of filtration system would be an "overbroad" limit on freedom of expression and would not survive a *Charter* challenge.

### **(B) Specific Implementation of Embedded Filtration Systems**

The possibility does exist for *embedded filtration systems* to be imposed in specific circumstances. It would probably be a reasonable restriction on freedom of expression for *embedded filtration systems* to be implemented for computers in public places specifically for the use of children. For instance, specifically chosen programs could be implemented in children's sections of libraries or in elementary schools.<sup>cvi</sup> "(T)he library would have to bifurcate filtered access to the net between children and adults. Filtering on the adult terminals would be limited ... while filtering on the children's terminals would be somewhat less circumscribed."<sup>cvii</sup>

### **(C) Filtration on a Voluntary Basis**

Such targeted restriction of Internet content would likely pass a *Charter*<sup>cvi</sup> challenge. This is far, however, from a blanket censorship system imposed on Canadian Netizens generally. Such a blanket regulation schema simply would not be constitutional for the reasons discussed.

Targeted restriction, however, would best be done at a private level rather than at a public level. Rather than imposing such a filtration system on society at large, the government could supply educators, librarians, parents and analogous groups with such programs to be used on a voluntary basis. Government regulations could be imposed on software manufacturers requiring Internet search programs to come equipped with the option to execute filtration programs like those associated with PICS as well as the option to try different compatible rating schemes.

## **(VI) Conclusion**

The justification for limiting access to Internet content is generally grounded in a 'community standards' argument. Offering a range of *embedded* filtration software rating systems to the public at large will give the option to the 'community' to filter content on a subjective basis. If Canadian 'Netizens' choose to implement such filtration programs and to filter out unrated sites, then site operators will be inclined to rate their sites and a market for rating systems will further develop. Conversely, if more sites are voluntarily rated, more Canadian Net surfers will have the confidence to filter out unrated sites without concern that they are missing important information. This will also encourage a market for rating systems, but only if the will of the community so dictates.

This form of laissez-faire "downstream"<sup>ci</sup>x filtration is currently the only means of regulating Internet content that would pass a Canadian *Charter*<sup>cx</sup> challenge. Such a means of filtration leaves the option of filtering to the dynamics of the Internet itself. If users want ratings and filtration then site operators will so oblige. If users, however, choose to forego any sort of ratings or filtration, then site operators will not make the effort to rate their sites, and this omission would be justified.

Such is the only fair and logical means to go about regulating the Internet. This new medium has evolved unregulated for nearly a decade and has attained a life of its own. It would be both unconstitutional, and practically inappropriate for legislators to attempt to regulate this medium now. The best role governments could take in this process of regulation would not be to impose regulation. The most appropriate role for government would be to help facilitate such filtration of content, if the will of the community tends in this direction. As regulation only tends to be justified on the basis of a 'community standard,' then it is only natural and appropriate to leave the means, limits, and even the existence of Internet regulation to the community itself.

**TABLE OF CASES**

*Miller v. California* 413 U.S. 15, 93 S.Ct.2607 (1973)

*R. v. Butler*, [1992] 1 S.C.R. 452

*R. v. Oakes*, [1986] 1 S.C.R. 103; [1986] S.C.J. 7

*R. v. Zündel*, [1992] 2 S.C.R. 731; [1992] S.C.J. 70

*Reno v. ACLU*, 117 S. Ct. 2329 (1997)

*Sable Communications of California, Inc. v. F.C.C.*, 127 S.Ct. 115, (1989)

## BIBLIOGRAPHY

- Communications Decency Act* 47 U.S.C.A. §223 (1996)
- Semmel, N.M. "Talking Back to Cyber-Mom: Challenging the Communications Decency Act of 1996" 1998 14 N.Y.L. Sch. J. Hum. Rts. 533
- Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11
- Criminal Code of Canada*, R.S.C. 1985, c. C-46, s.181
- Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11 at S.52(1)
- Hogg, P.W., *Constitutional Law of Canada*, 3d ed. (Toronto: Carswell, 1992)
- Lessig, L., "What Things Regulate Speech" (1998) 38 *Jurimetrics J* 629
- Meyer, C., "Reclaiming Sex from the Pornographers: Cybersexual Possibilities", (1995) 83 *Geo. L.J.* 1969
- Kuner, C., "Legal Aspects of Encryption in the Internet" *International Business Lawyer* (April, 1996)
- Resnik, P. & Miller, J., "PICS: Internet Access Controls Without Censorship" (1996) 10 *Comm. ACM* 87
- Wagner, R.P., "Filters and the First Amendment" (1999) 83 *Minn. L. Rev.* 755
- Ramsey, C.W., "Burning the Global Village to Roast a Pig: The Communications Decency Act of 1996 is not "Narrowly Tailored" In *Reno v. ACLU*" (1997) 32 (3d) *Wake Forest L. Rev.* 1316
- Oram, A., "Why I Do Not Install Filters On My Children's Computer" (October 27, 1998) [http://www.oreilly.com/people/staff/andyo/ar/filter\\_argument.html](http://www.oreilly.com/people/staff/andyo/ar/filter_argument.html) (last visited April 17, 1999).

## ENDNOTES

- 
- <sup>i</sup> *Communications Decency Act* 47 U.S.C.A. § 223 (1996). [hereinafter CDA]
- <sup>ii</sup> *Reno v. ACLU*, 117 S.Ct. 2329 (1997). [hereinafter *Reno*]
- <sup>iii</sup> *Id.*
- <sup>iv</sup> *Sable Communications of California, Inc. v. F.C.C.*, 127 S.Ct. 115, (1989).
- <sup>v</sup> *Supra* Note (ii).
- <sup>vi</sup> *Id.*
- <sup>vii</sup> N.M. Semmel, "Talking Back to Cyber-Mom: Challenging the Communications Decency Act of 1996" (1998) 14 N.Y.L. Sch. J. Hum. Rts. 533 at 566.
- <sup>viii</sup> *Reno*, at 2351.
- <sup>ix</sup> *Id.*
- <sup>x</sup> *Supra* Note (i).
- <sup>xi</sup> *R. v. Oakes*, [1986] 1 S.C.R. 103; [1986] S.C.J. 7. [hereinafter *Oakes*]
- <sup>xii</sup> *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11.
- <sup>xiii</sup> *Supra* Note (i).
- <sup>xiv</sup> *Supra* Note (xii).
- <sup>xv</sup> *Supra* Note (ii).
- <sup>xvi</sup> *Reno* at 2353.
- <sup>xvii</sup> *Supra* Note (xi).
- <sup>xviii</sup> *Supra* Note (xii).
- <sup>xix</sup> *Id.*
- <sup>xx</sup> *Id.* at s. 1.
- <sup>xxi</sup> *Supra* Note (xii).
- <sup>xxii</sup> *Supra* Note (xi).
- <sup>xxiii</sup> *Oakes* at 104.
- <sup>xxiv</sup> *Supra* Note (xi).
- <sup>xxv</sup> *Oakes* at 104.
- <sup>xxvi</sup> *Reno* at 2353.
- <sup>xxvii</sup> *Supra* Note (i).
- <sup>xxviii</sup> *R. v. Zündel*, [1992] 2 S.C.R. 731; [1992] S.C.J. 70. [hereinafter *Zündel*]
- <sup>xxix</sup> *Supra* Note (i).
- <sup>xxx</sup> *Supra* Note (xii).
- <sup>xxxi</sup> *Supra* Note (xxviii).
- <sup>xxxii</sup> *Criminal Code of Canada*, R.S.C. 1985, c. C-46, s. 181.
- <sup>xxxiii</sup> *Supra* Note (xii).
- <sup>xxxiv</sup> *Supra* Note (xi).
- <sup>xxxv</sup> *Supra* Note (i).
- <sup>xxxvi</sup> *Supra* Note (xii).
- <sup>xxxvii</sup> *Zündel* at 793.
- <sup>xxxviii</sup> *Id.* at 794.
- <sup>xxxix</sup> *Id.* at 795.
- <sup>xl</sup> *Supra* Note (i).
- <sup>xli</sup> *Supra* Note (xxxii).
- <sup>xlii</sup> *Supra* Note (i).
- <sup>xliii</sup> "Random Access Memory" (memory necessary to view images on a computer screen)
- <sup>xliv</sup> *Supra* Note (i).
- <sup>xlv</sup> *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11. at S. 52(1) which gives the Charter power to override other provisions.  
Also see P.W. Hogg, *Constitutional Law of Canada*, 3d ed. (Toronto: Carswell, 1992) at 903-4.

- 
- <sup>xlvi</sup> *R. v. Butler*, [1992] 1 S.C.R. 452.[ hereinafter *Butler*]
- <sup>xlvii</sup> Supra Note (i).
- <sup>xlviii</sup> This test was outlined in the case of *Miller v. California* 413 U.S. 15, 93 S.Ct. 2607 (1973). This judgment defined 'obscenity' according to a state-by-state standard. This standard was defined according to what will offend the community threshold of decency.
- <sup>xliv</sup> Supra Note (ii).
- <sup>l</sup> *Reno* at 2352.
- <sup>li</sup> Supra Note (xlvi).
- <sup>lii</sup> *Butler* at 493.
- <sup>liii</sup> Supra Note (xi).
- <sup>liv</sup> Supra Note (xii).
- <sup>lv</sup> Supra Note (i).
- <sup>lvi</sup> *Id.*
- <sup>lvii</sup> Supra Note (xii).
- <sup>lviii</sup> *Id.*
- <sup>lix</sup> Supra Note (xi).
- <sup>lx</sup> Supra Note (xii).
- <sup>lxi</sup> Supra Note (xi).
- <sup>lxii</sup> Supra Note (i).
- <sup>lxiii</sup> Supra Note (ii).
- <sup>lxiv</sup> *ACLU v. Reno*, 929 F. Supp. 824, 827 (E.D. Pa. 1996)
- <sup>lxv</sup> Supra Note (i).
- <sup>lxvi</sup> *Reno* at 2352.
- <sup>lxvii</sup> *Reno* at 2353.
- <sup>lxviii</sup> Currently available are programs from producers such as:  
Cyberpatrol; EdView; InterGO Communications Inc.; Internet Filter; Parent control software for NETCOM users; NetNanny; New View; Safe Surf; Surfwatch
- <sup>lxix</sup> Supra Note (i).
- <sup>lxx</sup> L. Lessig, "What Things Regulate Speech" (1998) 38 *Jurimetrics J.* 629 at 653. [Hereinafter *Lessig*]
- <sup>lxxi</sup> Such programs work by examining the content of a web site, looking for 'inappropriate' words or phrases. If these are found, the site is blocked from entering the user's computer.
- <sup>lxxii</sup> C. Meyer, "Reclaiming Sex from the Pornographers: Cybersexual Possibilities", (1995) 83 *Geo. L.J.* 1969 at 1988. [hereinafter *Meyer*]
- <sup>lxxiii</sup> For a further discussion of 'encryption' and the legal issues surrounding it see:
- <sup>lxxiv</sup> C. Kuner, "Legal Aspects of Encryption in the Internet" *International Business Lawyer* (April, 1996).  
<sup>lxxv</sup> *Meyer* at 1984.
- <sup>lxxv</sup> *Id.*
- <sup>lxxvi</sup> *Lessig* at 653.
- <sup>lxxvii</sup> Supra Note (xii).
- <sup>lxxviii</sup> Supra Note (i).
- <sup>lxxix</sup> P. Resnik & J. Miller, "PICS: Internet Access Controls Without Censorship" (1996) 10 *Comm. ACM* 87. [hereinafter *Resnik*]
- <sup>lxxx</sup> R. P. Wagner, "Filters and the First Amendment" (1999) 83 *Minn. L. Rev.* 755 at 760-761. [hereinafter *Wagner*]
- <sup>lxxxi</sup> "As of early summer 1998, it appears that there are six self-rating systems developed and several other third-party rating systems based on PICS. By far the largest of these is sponsored by the Recreational Software Advisory Council on the Internet (RSACi). In December 1997, RSACi claimed to have 50,000 pages of content rated according to its system and comes pre-installed in all versions of Microsoft's Internet Explorer." (*Wagner* at 761)
- <sup>lxxxii</sup> *Resnik* at 93.
- <sup>lxxxiii</sup> *Wagner* at 760.
- <sup>lxxxiv</sup> This type of user-based policing will also work to correct misratings for sites that were made accidentally; not only those made by unscrupulous site producers.
- <sup>lxxxv</sup> PICS has the potential to become very popular, even if used on a voluntary basis. It has the potential to aid in Net searches by, for instance, limiting the sites that are searched to sites pertaining to 'art collection'

or 'philosophy' or 'Elvis Presley,' etc. In this way, such a filtration system could be used, not only to censor, but to "edit" content for a user's convenience.

<sup>lxxxvi</sup> *Wagner*, at 761.

<sup>lxxxvii</sup> C.W. Ramsey, "Burning the Global Village to Roast a Pig: The Communications Decency Act of 1996 is not "Narrowly Tailored" In *Reno v. ACLU*" (1997) 32 (3d) Wake Forest L. Rev. 1316 at 1321. [hereinafter *Ramsey*]

<sup>lxxxviii</sup> *Id.*

<sup>lxxxix</sup> *Id.*

<sup>xc</sup> *Wagner* at 763.

<sup>xc</sup> *Supra* Note (viii).

<sup>xcii</sup> For an excellent argument against screening children from any Internet content whatsoever, see:

A. Oram, "Why I Do Not Install Filters On My Children's Computer" (October 27, 1998)

[http://www.oreilly.com/people/staff/andyo/ar/filter\\_argument.html](http://www.oreilly.com/people/staff/andyo/ar/filter_argument.html) (last visited April 17, 1999).

<sup>xciii</sup> *Supra* Note (lxxxvii).

<sup>xciv</sup> *Supra* Note (i).

<sup>xcv</sup> *Supra* Note (ii).

<sup>xcvi</sup> *Supra* Note (i).

<sup>xcvii</sup> *Supra* Note (xii).

<sup>xcviii</sup> *Supra* Note (lxxxvii).

<sup>xcix</sup> *Supra* Note (i).

<sup>c</sup> *Supra* Note (ii).

<sup>ci</sup> *Supra* Note (xii).

<sup>cii</sup> *Id.*

<sup>ciii</sup> *Supra* Note (lxxxvii).

<sup>civ</sup> *Id.*

<sup>cv</sup> *Id.*

<sup>cvi</sup> Such programs likely could not be implemented in all library computers without being an overbroad restriction on freedom of expression. Such legislation has been introduced in various American municipal jurisdictions and has been struck down as not constitutional. Restricting only children's access, however, has been found by American courts to be a reasonable restriction on free speech and would also likely be acceptable under the Canadian *Charter*.

<sup>cvii</sup> *Wagner* at 766.

<sup>cviii</sup> *Supra* at Note (xii).

<sup>cix</sup> *Supra* Note (lxxxvii).

<sup>cx</sup> *Supra* Note (xii).