Can the Internet Be Governed?

Introduction

The World's lawmakers continue to grapple with the question to what extent, if any, the Internet can be governed. The Internet presents both domestic and international lawmakers with a myriad of legal challenges in formulating rules, whether on an individual country basis, or on a cooperative international level. By its very nature, many of these challenges are logistical in nature. To even describe the Internet in an omnibus fashion is in fact to mis-describe it. In reality, the Internet is a labyrinth of many computer networks and thus lacks a focal point for the purpose of its regulation.

Part of the challenge is also posed by its meteoric growth. An estimated 300 million people now access the Internet. This is estimated to grow to more than one billion users by 2005.*1* Rapidly evolving technology is often outpacing technological measures aimed at curbing abuses.

The challenge to the lawmakers is also a philosophical one. One writer has noted that some commentators believe that "the Wild West anarchy in which the world computer network grew up will make it impossible to tame".*2* The Internet is the product of evolution, and not of planned development. Its almost lawless state is, to many, its greatest appeal.

From the beginning, the Internet had its own limited set of rules. When the Internet was primarily a vehicle for academia, users relied upon custom and "netiquette" to ensure that users observed the rules. In 1986, the National Science Foundation promulgated a policy of "acceptable uses". The Policy expressly prohibited for-profit activities, unless in furtherance of a specifically acceptable use.*3* However, the explosive and unregulated growth of the Internet meant that by the early 1990's, the Internet had clearly outgrown its origins.

As the Internet has grown and evolved, the challenge of its governance has grown to become a modern day leviathan. The founder of American Online Inc. (AOL), James Kimsey, was quoted in April 2000 about the ability of AOL to defend itself against hackers and whether certain countries could limit access to the Internet:

AOL as an institution probably has more experience in this interactive media than any other large institution in the world. We have battalions of programmers deployed against hackers and we're losing. I think Vietnam, China and others that are trying to control the Internet - even our own government - have no chance.*4*

To what extent these challenges can be resolved by international and domestic legal systems remains to be seen. The very essence of the Internet is the freedom of its users to connect and interact. This freedom is a veritable anathema to the regulator.

Background

The development of a worldwide computer network is primarily the result of an evolutionary process, rather than any coordinated international effort. To understand the challenges, it is first necessary to understand what exactly the Internet is. The Internet is based on the concept that there could be independent networks that could interact without regard to their particular network architecture. Networks would be able to interact with each other through a meta-level "Internetworking Architecture".*5* As a fundamental corollary to the method of the interaction, the global network would be based on an "open architecture" concept. Accordingly, there would be relatively few constraints on the types of networks that could interact with the global network.*6*

Initially, the Internet was not a commercial vehicle. Rather, the network was used primarily by academics and the military. Internet protocol addresses were simply assigned on a "first come", "first served" basis. As the number of host computers comprising the Internet grew, it became necessary to establish a system of identification. Previously, it had been possible to keep track of the hosts and their corresponding addresses simply by keeping track of their respective names. This led to the implementation of the "Domain Name System", which was invented by Paul Mockapetris of the University of Southern California.*7* This system facilitated the naming, distribution and organization of computer hosts connected to the Internet. The task of assigning Internet protocol numbers resided with the Internet Assigned Number Authority, a part of the Information Sciences Institute of the University of Southern California until October of last year.*8* Its role has now been supplanted by the non-profit corporation, the Internet Corporation for Assigned Names and Numbers (ICANN).*9* From the perspective of the legal scholar, it is noteworthy to observe that this development appears to have taken place without any meaningful consideration of regulation. Juxtaposed against this observation, it should be noted that much of the use of the Internet in its developmental stages, was focused on specific requirements, and not on a global vision.*10*

Similarly, changes to the software that are an integral part of the Internet have been provided on an open basis. Providers have historically willingly exchanged information and technology with a view to enhancing the overall level of connectivity and to promote ease of interaction.

The Pace of Change

The explosive growth of the Internet is undeniable. In 1989, the Internet had 100,000 host computers. By 1992, the number had increased to 1,000,000. The latest statistics indicate that there are now more than 53,000,000 hosts.*11* Moreover, access is not constrained by international affiliations, but rather is available to anyone with the appropriate technology. Accordingly, Western countries may be potentially held hostage to rogue nations, who either choose not to regulate the medium at all, or simply lack the resources

to regulate. A case in point is the Canadian experience with a web site operating out of Alberta under the moniker of the "World Stock Exchange". This site was operated without any government sanction. When securities regulators issued a cease trading order, the World Stock Exchange moved its host computer to the Cayman Islands. Thereafter, when the Government of the Cayman Islands expressed some concern that the site might mislead people in the Caymans, which was at the time developing its own stock exchange, the host computer was relocated to Antigua.*12* The message in this affair was that a country was almost powerless to shut down a web site, where its backers were prepared to forum shop until an accommodating jurisdiction could be found in which to locate its server.

Nowhere to Hide

Unlike any predecessor medium, it is all but impossible for a country to isolate itself from the Internet. The reality is that the Internet is changing how people interact and how countries interact. Concomitant to the foregoing, it follows that the legal regimes which govern this interaction must change. The Chinese Government has sought to implement controlled isolation by erecting the "Great Firewall of China."*13* Although purportedly intended to stop Chinese citizens from accessing pornography and avoid paying taxes, it was clear that the real agenda was to quell potential civil unrest.*14* The reaction of the Chinese Government is case in point of the power of the Internet. The ability of governments to manage the dissemination of information is rapidly being eroded. The Chinese Government is fighting a battle that it cannot possibly win in the end. To date, the development of the Internet has often outpaced the ability of governments to regulate it.

Telecommunications

Historically, the regulation of radio, television and other media has been an integral part of a country's cultural framework, as manifested through its edifice of national laws and corresponding regulation. Canada is an excellent case in point. In Canada, regulation of telecommunications is a federal matter. The regulatory body is the Canadian Radio-television and Telecommunications Commission (C.R.T.C.).*15* Although Canada has been one of the strongest proponents of liberalized trade in general, Canada has supported numerous exceptions and qualifications provided for within the General Agreement on Trade in Services (GATS). These limitations reduce the scope and broaden the time-frame for the liberalization of the regulation of telecommunications in the World.

Historically, regulation of telecommunications has been based upon the various types of media. In other words, television and radios were distinct, telephones were distinct from cable, and all forms of media were distinct from newspapers. Each medium was in turn overseen by a different regulatory body. With the commercial development of the Internet, the distinction is becoming increasingly blurred. The ability of the Internet to provide the framework for the delivery of telephone, television, radio and computer communications is termed "convergence". The convergence phenomenon is already providing a practical constraint on the ability of countries to regulate the media

In Canada, the C.R.T.C. has refused to regulate the content or the provision of television and radio type services via the Internet.*16* Rather, the role of the C.R.T.C. in this area has been, to date, largely to act as an arbitrator in determining whether certain Internet providers would have access to high speed cable providers, and if so, at what price.*17* Perhaps this is an implicit recognition of the inherent difficulty associated with regulating the Internet in the so-called "Global Village". The recent litigation brought against upstart iCraveTV, which established an Internet site to broadcast various American and Canadian television stations without first obtaining license agreements, provides some proof that the marketplace can, at least in certain circumstances, regulate itself.*18* That being said, the iCraveTV case is also testament to the powerful deterrence that can arise from litigation commenced in the United States, from the standpoints of both costs and uncertainty of outcome.

Commerce

The growth in commerce over the Internet has outpaced the development of a coherent set of rules to regulate the conduct of business through this medium. Many promoters of Internet commerce have suggested that a "new regulatory framework" is needed to cope with this burgeoning area.*19* There are a variety of issues in this area. However, as a preliminary comment, the analysis must differentiate between transactions between businesses and those involving consumers.

Turning firstly to business to business, the paramount consideration is the development of a coherent set of rules governing the commercial interaction of businesses on the Internet. Most commercial lawyers will not object to "bad laws", provided they are applied universally with an option allowing the contracting parties to opt out and apply their own rules. In contrast, commercial lawyers will object to rules that are uncertain. Uncertainty adds needlessly to the cost of transacting and may actually deter enterprises from availing themselves of potentially the lowest cost method of carrying on business available to them.

In the business to business context, the Internet has already achieved a remarkable level of self-regulation. One key aspect to business via the Internet is the necessity of verifying with whom we are contracting and verifying the consent when given. The technological response of developing and maintaining a satisfactory level of encryption is a business imperative. As noted by Jane Winn:

Commercial law is in the process of adapting to meet the challenges posed by electronic commerce conducted over open networks. Authentication procedures are an essential element in the security policies and procedures that will be essential to the commercial exploitation of the Internet.*20*

With respect to business to consumer transactions, the argument that the marketplace can self-regulate is much less compelling. Unlike business to business transactions, the consumer may not be able to negotiate the terms of the bargain, as most transactions of this sort will be contracts of adhesion. Businesses transacting via the Internet will be at liberty to "forum shop", in the absence of a coherent international set of rules governing consumer transactions. As well, businesses located in less restrictive jurisdictions will enjoy a competitive advantage over their counterparts elsewhere, thereby exacerbating the risk that a consumer might transact with a less than reputable merchant.

The principal consideration to date has focused on what is the electronic equivalent of the signature. In Canada, the Province of Saskatchewan has become the first jurisdiction to implement legislation governing the electronic signature. The legislation is similar to laws recently enacted in California and Pennsylvania.*21* Yet even in the domestic context, the Saskatchewan Justice Minister had to concede the limited effect of the initiative:

The problem is that e-commerce and the Internet are border-less, so the impact of the legislation in a single province is limited. We won't see the real impact until all of the provinces sign on [emphasis added].*22*

If there is recognition that the legislation has only a limited impact in the domestic context, there can be little doubt as to even more limited efficacy of the Saskatchewan legislation in an international context.

Hyperlinks

The process by which one web site is linked to another is what is referred to as "hyperlinking". Hyperlinking was originally designed to allow academics to link to another scholarly paper.*23* However, with the increasing commercial exploitation of the Internet, hyperlinking is now used primarily as a vehicle to direct users from one commercial site to another.

Hyperlinking presents a useful microcosm in assessing the extent to which the Internet is capable of being regulated. The rights of individual web site owners are limited by the Internet's embracing of the unrestricted flow of information. The contrast in perspectives is made abundantly clear in the following quotes:

Web inventor Tim Berners-Lee: When you make a bookmark or a hypertext link, you should be able to make that link to any piece of information that can be assessed using networks.

New York attorney Emily Madoff: There is no legal authority that says you are free to link to someone else's Web site.*24*

The foregoing debate highlights the inherent tension between those who oversaw the creation of the Internet and the desire on the part of the legal community to graft onto the Internet certain laws and regulation.

The first time a linking dispute was litigated happened in late 1996 in Scotland. The Shetland News began to link stories to its rival, The Shetland Times. The context in which the links were made were regarded as potentially offensive to The Times. The Times sued claiming a violation of its copyright. An injunction was granted on an interim basis precluding the linking. The case ultimately settled prior to a final disposition of the matter.*25* It is widely believed that an American court would not have even allowed the case to proceed as far as it did.*26*

The legalities of hyperlinking are currently being examined in an American context in the case of Ticketmaster v. Tickets.com.*27* Ticketmaster allows consumers to purchase tickets to various events with which it has various exclusive arrangements. Tickets.com also allows consumers to purchase tickets, but also provides information as to how consumers can purchase tickets that are not available through it.

Visitors to the Tickets.com web site are invited to click on "Buy this ticket from another on-line ticketing company" when the tickets are not available through Tickets.com. If the user so clicks, he is instantly transferred to another ticket agency, in many cases that of Ticketmaster. The interior Web page then accessed by the consumer contains the Ticketmaster logo.*28* In an interim ruling, the Court concluded without equivocation that Tickets.com's hyperlinking did not constitute a violation of Ticketmaster's copyright.*29*

Protecting the Rights of Intellectual Property Owners

The Internet poses a tremendous threat to the rights of the owners of intellectual property. The advent of the digital age is challenging copyright in a number of ways. In a report prepared by the U.S. Congressional Office of Technology Assessment, six different challenges were noted:

Digital works are easily copied, with no loss of quality; they can be transmitted easily to other users or be accessed by multiple users; they can be manipulated and modified easily and changed beyond recognition; works treated very differently under current copyright law are essentially equivalent: text, video or music are all reduced to a series of electronic "bits" and stored in the same medium; works are inaccessible to the user without hardware ad software tools for retrieval, decoding and navigation; software allows for new kinds of search and linking activities that can produce works that can be experienced in new ways, e.g. interactive media.*30*

The best case in point to date evidencing the technological threat involves the music recording industry. The rapid development of MP3 technology has already had a dramatic impact upon the recording industry. Consumers can download music from the MP3.com site, simply by certifying that they are already the owners of a compact disk

with that song. A new generation of players has developed to allow listeners to play back their MP3 recordings.

MP3.com was the defendant in litigation brought against it by the Recording Industry Association of America. Although the litigation was successful against MP3.com, there can be little doubt that the technology available through the Internet will profoundly affect the music industry for the foreseeable future.*31* In the near future, faster Internet access for consumers will similarly alter the future of the video business.

Protecting the rights of trademark holders has always been a challenge outside Western countries.. Many nations lack either the formal legislation protecting trademark holders, or the will (or perhaps resources) to defend the rights of intellectual property holders. This problem is magnified when a consumer in the West has, through the Internet, instantaneous access to web sites in jurisdictions that do not protect the rights of trademark holders.

A few commercial enterprises are, in the absence of any international effort, attempting to fill the regulatory breach. Napster, a software program that allows users to download and share MP3 files (i.e. in most cases, songs) has been the subject of litigation by disgruntled musicians. The band Metallica has recently delivered a list of users to be banned from accessing Napster. These users are alleged to have downloaded the Band's songs in contravention of the Digital Millennium Copyright Act. Banned users may submit in response a "counter notification" form. In the event Metallica does not pursue legal action against the user within ten working days, the user will be reinstated.*32* As a practical reality, there can be little doubt that many of the users of Napster are accessing and downloading files from the web site in violation of copyright laws. However, the isolated actions of a few musicians is unlikely to provide, at least in any material way, any level of self-governance. To exacerbate matters, at least from a copyright perspective, the perceived villain among Internet users is, in my view, Metallica, and not Napster.

Criminal Law

Regulation of international criminal activity has always presented great challenges to lawmakers. What makes the Internet different is the accessibility and the relative freedom to move to other jurisdictions. Many jurisdictions either have more relaxed laws regarding so-called "cyber-crimes", or possibly no rules at all. The recent "I Love You" virus has been traced to one or more individuals in the Philippines. However, under the law of the Philippines, it is not clear what crime has been committed. Charges may be laid under the Access Devices Regulation Act of 1998, but that would appear to allow a potential defense that no secret information was obtained from other web sites. This legislation was enacted to make it a criminal offense to obtain credit card and other personal information for a fraudulent purpose. Importantly, hacking per se does not appear to be a criminal activity under the penal laws of the Philippines.*33* This led to calls to extradite the alleged perpetrators to the United States of America for prosecution. However, it may well be difficult to extradite a citizen to a foreign country for an activity

not regarded as criminal in the domestic country. The extradition process is premised upon an extradition treaty which sets forth what crimes an individual can be extradited for.

The Internet allows cyber-criminals to target victims in another jurisdiction. Moreover, access to programmes that camouflage the actual user (or more typically users) add to the enforcement woes of police forces around the world. The specter of global cyber-warfare, perhaps at the corporate level or even plausibly between countries, is perhaps the most compelling area necessitated a coordinated global effort. The web site of the Hizbollah had long been the target of the Israeli government. In the early stage of the web site, the Mossad would orchestrate a number of simultaneous "hits" on the site, thereby precluding access by other users.*34* To what extent a web site is fair game in the context of an actual armed conflict is a legitimate question. One thing is clear however, there are presently no rules of engagement governing this type of conflict.

That being said, a consensus is evident that the strategy of inundating a web site with hits is criminally actionable in the commercial and government contexts. The arrest and prosecution of Mafiaboy demonstrated a high level of cooperation, at least among Western nations, to bring the perpetrator to justice. Mafiaboy is remembered as the Canadian teenager who brought a number of web sites to a virtual standstill.*35* Lost on most commentators though, legal as well as technical, was the extraordinary vulnerability of the entire network. If a fourteen year old Canadian boy could bring cnn.com (by way of an actual example) to a standstill, imagine what a competitor could do. Then, imagine what a terrorist organization could do. And then lastly, imagine that the perpetrators decide to launch the attack from a jurisdiction that was not prepared to cooperate with Western law enforcement agencies.

Where Jurisdictions Overlap

Just because an activity is illegal in one jurisdiction does not, obviously, make it illegal in another jurisdiction. In the Internet, a world without borders, the rules that seem to apply are that of the most laissez-faire entity having jurisdiction. One case in point in this regard is the veritable explosion of "Internet Gambling". The market for Internet gambling was "guesstimated" in 1997 at $1.8 billion (United States currency) and was estimated to grow to $8.6 billion in 2000.*36* This exponential growth has been realized notwithstanding either a judicial vacuum in some Western countries, or even legislation making such sites illegal. Most Internet gaming operations have been established to take advantage of the legal vacuum. As noted by Chris Generalis, in a report prepared for the United States Congress on gambling on the Internet:

Internet wagering pioneers contend in chorus that the existing law does not apply to them. Furthermore, that the US- as a single country- does not have the right to regulate the Internet, which is a worldwide entity. The typical cyber-bookie isn't even an American citizen and runs his gaming operation in a fashion typical of on-line setups: although operating primarily in the US, it's officially headquartered offshore with a foreign government's permission and license.*37*

This issue is a microcosm of the entire problem surrounding the governance of the Internet. Even in jurisdictions with the willpower and resources to deal with an issue, there remains the issue of what happens in the absence of international cooperation. Based on an analysis of the flourishing Internet gaming business, the reality is that an industry is able to develop without any practical restrictions whatsoever, provided that it is domiciled offshore in a cooperative jurisdiction.

Of course, businesses themselves can choose to adhere to self-imposed guidelines. With respect to enterprises like cyber-casinos, this may be the best practical hope for governance. Although one might ask why a proprietor of an offshore casino on the Internet would agree voluntarily to adhere to certain guidelines, there are compelling commercial reasons why they might choose to do so. Firstly, adopting guidelines would likely boost confidence with the patrons of the Internet casino, thereby encouraging more wagering among existing customers. Secondly, reputable casinos will be afforded a marketing edge over their less than honorable counterparts. Thirdly, reputable casinos will agree to preclude access to minors.

The Interactive Gaming Council (the "IGC") has been established a voluntary standard of conduct to which its members have agreed to adhere.*38* As of May 26, 2000, there were 53 full members and 37 associate members of the IGC. It is interesting to note that part of the mandate of the IGC is to promote the interests of the interactive gaming industry. Yet even though part of its role is to advance the business interests of its members, that in and of itself does not appear to be antithetical to the interests of the public. Rather, the public interest appears to be well-served notwithstanding the ostensible level of self-interest of the members of IGC. The mission of the Interactive Gaming Council is stated at its web site:

* Provide a forum for interested parties to address issues and advance common interests in the global interactive gaming industry;
* To establish fair and responsible trade guidelines and practices that enhance consumer confidence in interactive gaming products and services; and
* To serve as the industry's public policy advocate and information clearinghouse.*39*

It is my view that industry self-regulation is likely the only near term solution for regulating Internet gaming. Further, given the potential for abuse and malfeasance in this area, the efforts undertaken by the IGC are to be lauded.

Regulating Obscenity

Pornography is hard to miss on the Internet. Prolonged use of any search engine will almost invariably lead the user inadvertently to a web site featuring adult entertainment. For those seeking out this form of entertainment, the Internet offers a veritable

cornucopia of choice. Unlike other forms of media, there is essentially no regulation. This is in sharp contrast to television and radio, which of course are highly regulated.

A central feature of the obscenity laws in most Western jurisdictions is a consideration of local community standards. Putting the test in a succinct fashion, will the local community be offended by the dissemination of the material?*40* The problem presented by the Internet is thus that the standard of obscenity potentially becomes that of the most tolerant community. Those entering adult sites are typically asked to certify that they are older than eighteen years of age and that the material they will view does not violate their local community standards.

To some degree at least, technology may facilitate self-governance. Commercially available software will allow parents to restrict access to adult oriented web sites.*41* Moreover, countries can make individuals liable for viewing the material, in addition to disseminating it. Many countries with Islamic laws, such as Saudi Arabia and Iran, have specifically targeted the Internet.*42* However, the efficacy of such laws remains debatable. Moreover, students from these countries, studying abroad, enjoy unfettered access to the Internet.

Laws governing censorship invariably lead to a discussion about censorship and the dissemination of other undesirable material. While most Western jurisdictions note that freedom of speech does not extend to material considered to be obscene, the very examination of the issue tests the desire to balance competing rights. The Internet in many respects represents the ultimate in freedom - the freedom to publish, be seen and be heard. Such freedom is undoubtedly seen as destabilizing to many countries. If such freedom is an anathema to some countries, it is embraced by others. The result is that a coordinated approach on obscenity seems unlikely.

What's In a Name?

Perhaps no other area of Cyber law conflict has attracted as much attention as the various battles for domain names on the Internet. The so-called "dot.com" registration is administered by an American business known as Network Solutions.*43* Network Solutions is a public, for profit, corporation which also oversees the allocation of the suffixes "dot.net", "dot.org" and "dot.edu". Nay of the battles play out as epic struggles between "David" and "Goliath". Making matters even more interesting, some battles involve long time holders of a domain name against trademark holders.*44*

In most other jurisdictions, the allocation of Internet names is the responsibility of a non-profit entity or government agency. The agency seized with this task is more likely to be the product of chance evolution, rather than any significant regulatory aforethought. Canada is a case in point. The "dot.ca" registration system in Canada is administered by the Canadian Name Domain Name Consultative Committee, a non-profit entity.*45* In

fact, until recent proposed changes are implemented, there remains no charge for registering a "dot.ca" domain name.

Whether or not the role is handled by a non-profit entity or a public corporation, it is clear that these agencies are required to play a quasi-judicial role from time to time. The decision to allocate or revoke a registration of a domain name is clearly more than simply an administrative task. In such an exercise, a compelling case is made out that the agency must adhere to the rules of natural justice, or face judicial censure and possibly damages in a civil law suit.

Recognizing the role it sometimes is required to play, Network Solutions states at its web site that it advocates "a governance structure within a legal framework to help safeguard critical operations of the Internet".*46* Presently, Network Solutions takes a name out of service until the parties resolve their differences, whether through litigation, arbitration or negotiation.*47* Thus a legitimate rights holder to a domain name is effectively unable to obtain interim relief pending judicial resolution.

The problems associated with resolving domain name disputes has been recognized by the World Intellectual Property Organization, a United Nations agency (WIPO).*48* WIPO established the Arbitration and Mediation Center in 1994 to deal with commercial disputes. As part of its mandate, WIPO has developed the Uniform Domain Name Dispute Resolution Policy for the resolution of domain name disputes. The Center currently provides services in respect of the following suffixes: .com, .net, .org, .ac, .io, .nu, .sh, .tv and .ws. The Policy was adopted in October of last year by the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit entity that is assuming the administration of the Internet's addressing systems.*49*

The Arbitration and Mediation Center recently ruled in favor of actress Julia Roberts in a dispute with Russell Boyd over the domain site, The Center ruled that Ms. Roberts has common law trademark rights to the name and that the site was "identical or confusingly similar" with her name. Further, the site was registered in "bad faith", citing the fact that Mr. Boyd had registered the names of other celebrities. As well, the domain site was for sale on eBay Inc., an Internet auction service.*50*

The arbitration system does not preclude access to the courts, likely a concession to American interests. However, given the potential multi-jurisdictional aspect of a dispute, parties may be loathe to litigate the matter in addition to arbitrating it. Further, as with any administrative tribunal, the Center brings a greater level of expertise than would be found in the Courts. As the Center gains acceptance, it is likely that a universal and coherent approach to settling disputes over domain names will emerge.

Going It Alone

There is also the strategy of a country "going it alone", and prescribing penalties that apply without regard to jurisdiction. The one country that would appear to be able to make a material impact upon the Internet with such a strategy is the United States of

America. In November 1999, President Clinton signed into force the Anticybersquatting Consumer Protection Act. This legislation allows trade-mark holders to bring a civil law suit against cybersquatters. In addition to remedies available against parties that are subject to the jurisdiction of an American court, the Act creates an action in rem against the domain name itself where the domain name registrant is not subject to the jurisdiction of any United States federal court.*51* As most meaningful domain name registrations are "dot.com's", this initiative may well act as a deterrent to future cybersquatters, regardless of their locale.

Towards a Coordinated International Regulatory Effort

Janet Reno, the Attorney General of the United States, stated that "it is now clear that crime on the Internet, crime in terms of hacking, crime in terms of those that would use the medium in the wrong way...will require an international effort".*52* Activities historically regulated at the national level will, out of sheer necessity, require some level of international supervision. The case of the nascent World Stock Exchange speaks to the need to regulate the sale of securities over the Internet, without regard to national boundaries.*53*

In May 1998, the World Trade organization adopted a "Declaration on Global electronic Commerce". In this Directive, the General Council of the World Trade Organization was directed to "establish a comprehensive work programme to examine all trade-related issues relating to global electronic commerce".*54* However, after the meeting of the World Trade Organization in Seattle this past November, the status of the Declaration was left in doubt. Nonetheless, the Directive will undoubtedly be raised in future negotiations.

One important issue that will be at the forefront of consideration at the World Trade Organization is the extent to which electronic transmissions fall under the rubric of the General Agreement on Tariffs and Trade ("GATT") or the General Agreement on Trade in Services ("GATS"). The principal of non-discrimination enunciated under GATT is not mirrored in the GATS. This distinction is important in assessing the degree to which international regulatory oversight will be possible. That being said, there appears to be a clear agenda to move forward to establish international rules governing electronic commerce, with such negotiations being mandated by the existing trade rules.*55* However, as with most initiatives by the World Trade Organization, one should expect the progress to be torturously slow.

Prediction for the Future

The World is witness to an overall decline in the role of government in society. Even in societies that hitherto embraced bureaucracy, we are seeing a retrenchment. Concomitant to the foregoing, the Internet is expanding in what seems like a complete regulatory vacuum.

To some degree, controls will develop out of commercial necessity. For example, the online gaming industry has itself recognized the need for regulation, and the Interactive Gaming Council is a logical step in that direction. To eschew any regulation in this area would be to invite an international crackdown. Whether self-regulation in this area will suffice in policing cyber-casinos can certainly be questioned. Nonetheless, the development of the Council is an impressive first step.

Moreover, businesses themselves will likely create a workable set of rules to govern their contractual relationships. As businesses become increasingly multi-jurisdictional, one could expect that the World Intellectual Property Organization's Arbitration and Mediation Center will play an expanded role. Although the Center is from one perspective, a bureaucracy in itself, it is really more analogous to a private regulated body. Accordingly, it may prove better suited to coping with rapid technological changes than the traditional judicial systems.

The governance of the Internet is more problematic vis-a-vis the consumer. Technological improvements will provide, at best, only a partial solution. The marketplace will, at least to some degree, regulate itself. Consumers will migrate to reputable merchants in jurisdictions with consumer protection laws. The World Trade Organization has established a clear agenda to establish rules that will govern electronic commerce. The Anticybersquatting Consumer Protection Act may demonstrate that an initiative by a single country can, at least in a specific context, aid in regulating activity on the Internet.

Conclusion

The development of rules governing the Internet and the enforcement of those rules will be primarily an evolutionary process. I believe that the process will be much like the transformation of the Internet from a medium catering to the military and the academic world into a commercial medium. The rules will, to a very large degree, reflect the laissez-faire environment they were developed out of. The process will not be perfect; there will be gaps. There will not, however, be a complete failure to establish rules as envisioned by AOL founder, James Kimsey.

Much like a shopper at a souk, the user of the Internet will be bombarded with almost endless choice and confusing possibilities. The Internet is already the ultimate free market. Powerful economic and technological forces will ultimately limit the extent to which the Internet can, and will be, effectively governed. They will not however, completely preclude its governance. Rather, these same forces will ensure that some rules are in place in order assure the future technological and economic viability of the Internet. The answer to the question, "Can the Internet be Governed?" - is yes, albeit to a limited and hence imperfect extent.

Bibliography

David Brunnstrom, *No Country can Control the Web: AOL Founder*, (The Globe and Mail - April 27, 2000) , page T2.

Charles S. Clark, *Can the Use of Cyberspace be Governed?*

George Darby, *Integrated Internet Digital Networks: The Post-Convergence, Pure-IP Network Model.*
Http://207.26.203.164/archives/planetptc/papers/Darby_George/paper.htm

Keith Dawson, *An Inalienable Right to Link?*

Chris Generalis et al., *Internet Gambling.*

Green Paper on Convergence of Technologies (**The European Commission**).
Http://www.fabrimetal.be/sectoren/ict/news/12/convergence-ectel.htm

John Grimmett et al., *Clashing Domain Names Underlie Unusual Court Case.*

Information and Technology and E-Commerce Newsletter (**Canadian Bar Association - Ontario**) (December 1999).

Information Technology and E-Commerce Newsletter (**Canadian Bar Association - Ontario**), Volume 1, Number 2.

Jane Kauffman Wynn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 Tulane Law Review 1177; also:

Barry M. Leiner et al., *A Brief History of the Internet*,

Brad A. Myers, *Computer Almanac.*

John Partridge, *Julia now the Mistress of her Own Domain*, (The Globe and Mail - June 1, 2000).

Will Rodger, *Prices for Domain Names Surge.*

Jason Romney, *Who Can Stake a Claim in Cyberspace - Domain Names & Trademarks.*

Rules for Assignment of Domain Names.

Todd Spangler, *Critics Think Domain Names Plan is Unfair.*
Http://www.zdnet.com.filters/printerfriendly/0,6061,392422-35,00.html

Daniel Tobias, *Master of Your Domain.*

Fred L. Wilks, *The Community Standards Conundrum in a Borderless World.*

Citations

1.
2. Charles S. Clark, Can the Use of Cyberspace be Governed?. See at page 1.
3. Ibid, page 16.
4. David Brunnstrom, No Country can Control the Web: AOL Founder, (The Globe and Mail - April 27, 2000) , page T2. See also:
5. Barry M. Leiner et al., A Brief History of the Internet, at page 4.
6. Ibid.
7. Ibid at page 7.
8. See at page 3.
9. Infra, footnote #47.
10. Op. cit, footnote #2 at page9.
11. at page 2
12. See (also,)
13.
14. Ibid.
15. The C.R.T.C.'s web site can be found at:
16. In any event, Section 2 (c) (i) of the Annex on Telecommunications in GATS specifically excludes measures affecting the distribution of radio and television programmes.
17.
18. See A number of interested parties sought an injunction to take iCraveTV off the air. One wonders however, what might have transpired if iCraveTV had simply relocated its server from Canada to another jurisdiction.
19. Jane Kauffman Wynn, Open Systems, Free Markets, and Regulation of Internet Commerce, 72 Tulane Law Review 1177 at page 1. See also:
20. Ibid, page 41.
21. See (The Act itself can be found at).
22. Ibid, page 4.

23. Information and Technology and E-Commerce Newsletter (Canadian Bar Association) (December 1999) at page 8.
24. See at page 1.
25. See
26. Op cit., footnote #15 at pages 1-2.
27. U.S. District Court, Central District of California (March 27, 2000). See Http://www.gigalaw.com/library/ticketmaster-tickets-2000-03-27.htm
28. Ibid, page 2.
29. Ibid, page 3.
30. Office of Technology Assessment, "Information Security and Privacy in Network Environments," September 1994, page, taken from a 1992 OTA report, "Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technological Change." Infra, footnote #2, page 27, which refers to this excerpt.
31. See
32. See
33. See
34. See
35. Mafiaboy recently pled guilty to a number of offenses under Canadian law. See Http://ca.dailynews.yahoo.com/ca/headlines/cpress/ts/story.html?s=v/ca/cpress/20000517/ts/national_566028_1.html
36. Chris Generalis et al., Internet Gambling. at page 2.
37. Ibid, at page 5.
38. See
39. Ibid.
40. Fred L. Wilks, The Community Standards Conundrum in a Borderless World.
41. e.g. Net Nanny.
42. See
43. See
44. For example, CBS (owner of the Nashville Network) sued The Network Network over its domain site, The Network Network had registered and used the site since 1994. A complete synopsis of the case is found at the Network Network site. P.S. David beat Goliath in this case.
45. See
46. Op. Cit., footnote #38.
47. See Http://www.zdnet.com/filters/printerfriendly/0,6061,392422-35,00.html
48.
49. See

50. John Partridge, Julia now the Mistress of her Own Domain, (The Globe and Mail - June 1, 2000) page B12.
51. Robert L. Percival, Cybersquatters Thwarted with U.S. Anticybersquatting Consumer Protection Act, Information Technology and E-Commerce Newsletter (Canadian Bar Association - Ontario), Volume 1, Number 2 at pages 3 and 4.
52. Op cit., footnote #29, at page 2.
53. Infra., footnote #12.
54. Jennifer Chandler, Electronic Commerce and International Trade Rules, Information Technology and E-Commerce News (Canadian Bar Association - Ontario), Volume 1, Number2 at page 8.
55. Ibid, at page 9.