Canadian Journal of Law and Technology

Volume 1 | Number 3 Article 1

8-1-2002

Solving Legal Issues in Electronic Government: Jurisdiction, Regulation, Governance

John D. Gregory

Solving Legal Issues in Electronic Government: Jurisdiction, Regulation, Governance

John D. Gregory†

Introduction

Electronic communications are changing the world in radical ways because of the increase in value of information, the ease by which digitization transforms some kinds of things into data, the malleability of data, and their mobility in a system where borders tend to disappear.[1] A number of challenges arise for government that question its ability to govern and its character as we have come to know it. At the limit, it can be said that many governmental questions for the electronic age are being decided not by politicians, or even by traditional power elites, be they economic or military, but by engineering consortia, to some extent self-appointed and, up to recently, little known.

This paper looks at who can be governed, what can be governed, and how it can be governed in an electronic world. Whether law aims to be enabling (i.e., confirming the ground rules and the legal effectiveness of general conduct) or normative (i.e., imposing standards of conduct on more or less willing subjects), the new media presents difficulties for its rational evolution.

These are distinct questions from those raised by government online.[2] Electronic service delivery issues tend to focus on how government can carry on its traditional programs using electronic means and how the law can support it in doing so. The programs themselves evolve through the changing media, but not so much that they stop being recognizable. The transformation of government to deliver services electronically is just beginning, and the changes are not yet dramatic.

Here we start with a view of "jurisdiction", which considers how governments can regulate private conduct, whether in resolving disputes, protecting consumers, or repressing criminal or other offensive behaviour. The discussion looks at the courts and other dispute resolution methods, administrative processes, and alternative means to achieve the goals that have traditionally been sought by systems of direct commands and penalties. We then look at questions of the role of government faced with an electronic economy, particularly monetary and fiscal policy and taxation in general. The impact of electronic communications on the functioning of the democratic system is next: electronic publication of laws, electronic voting, governance models and public expectations. Finally, we review how technical rules and standards affect conduct that has been the purview of government, and some of the technical standards bodies whose role becomes more important in the electronic age.

Legal developments in these fields are more recent than those in electronic service delivery, and they are more affected by developments in technology. The categories of analysis used here are not yet fixed. Some hints of their evolution can be seen, however, and those with an interest in government have some obligation to try to discern where and how to act when appropriate.

Jurisdiction

Resolving disputes

One of the earliest functions of government was to resolve disputes between its subjects. Few, if any, governments lack a system of courts for this purpose. Courts have counted on the power of the state to enforce their rulings, and that power physically extended as far as the power of the state itself, which is to say, to the borders of the state and no further. Communications, personal movement and commerce between states have, for many years, presented challenges to the application of law and the competence of courts based in one state. Doctrines of law to decide who gets to hear disputes and whose law applies have a long history.[3] Over the years, an array of bilateral or multilateral arrangements have also been made to enforce judgments made in other states,[4] and that work continues to this day.[5]

Electronic communications have exacerbated these challenges. Both the volume and the nature of communications have changed. The number of electronic messages sent over the Internet is in the billions each

†General Counsel, Policy Branch, Ministry of the Attorney General, Ontario. This paper was developed from a presentation sponsored by the Centre for Innovation Law and Policy at the Faculty of Law, University of Toronto. The views expressed are not necessarily those of the Ministry or of the Faculty. Thanks to Troy Harrison, Charlotte Judd, Rhonda Lazarus, Jinyan Li, Michael Power, Jeanne Proulx and Karen Wold for their helpful comments on versions of this paper, and to Mark Ratner and Kajal Khanna for tracking down some necessary notes.

year.[6] The nature of the Internet is that any computer connected to it can be accessed by any other computer connected to it. Information is available on a "pull" basis, meaning that the person wanting information has to "go" and get it, by requesting that it be sent. Cross-border transactions nowadays run particularly on the World Wide Web, which makes this kind of communication very easy. However, developments in commercial practices and in web technology complicate the picture, so that "push" techniques are also known, by which people receive information or offers at the initiative of the sender, whether by prior subscription or by some other form of selection.

Through the courts

What disputes about electronic communications are properly before the courts of any one place? Courts have been wrestling with this subject for several years, and lawmakers in some places more recently. Most of the judicial decisions have come from the United States. This is not the place to canvass the trends in detail. Suffice it to say that courts have become more subtle in their reasons for deciding to take or not to take jurisdiction over online disputes.[7] For a while, a consensus formed around what was called the "active/passive" test associated with the *Zippo* case.[8] A court would take jurisdiction if the electronic communications offered active engagement in a transaction in the territory of the court. Passive communication, merely making information available, was not enough. This approach was adopted by the British Columbia Court of Appeal in *Braintech v. Kostiuk*,[9] in which the Court refused to enforce a Texas judgment against a defendant resident in British Columbia on the ground that the Texas court had not properly taken jurisdiction over the case.

More recently, the active/passive test has been questioned, partly because not all cases are going that way, and partly on principle.[10] As Internet commerce becomes more interactive, merchants doing business online would be exposed to an increasing number of courts and legal regimes, whether or not they really wanted to do business in all the territories from which their sites may be reached. Professor Geist proposes a "targeting" principle, based on an "effects test": where was the communication intended to have an effect, both subjectively (depending on the targets the merchant had) and objectively (whether it was reasonable to expect the communication to have an effect).[11]

To some extent, questions of law and forum have been answerable by parties to transactions, who can choose such matters by contract, subject to limits imposed to protect vulnerable parties or for public policy reasons.[12] Such choices can be made online, and at least one Ontario court has enforced that choice.[13] The law on what is allowable by contract does not need to change very much because of the medium. The same is true for the law applicable to the dispute, once the court has taken jurisdiction.

The work of The Hague Conference on recognition and enforcement of judgments has been mentioned.[14] From 1998 through 2002, the working group paid a good deal of attention to the impact of electronic communications on its principles, but without resolution. The discussions became more complicated lately because holders and users of intellectual property have argued that intellectual property rights in one country might be enforced through a Hague Convention in another country, even if the policy balance of IP rights in the enforcing country were different. Concerns were expressed as well about enforcement of judgments that affect free speech differently in different countries.[15] In the spring of 2002, the Conference decided to defer work on electronic aspects of jurisdiction, to focus on "core" principles.[16]

Pending some resolution of these difficult questions at the international level, there is little role for domestic law reform on the jurisdiction question in civil matters.[17] The interprovincial borders in Canada are no more porous than the international borders. The law of jurisdiction in Canada itself has been restated by the Supreme Court of Canada in recent years.[18] The principle has been embodied in uniform legislation, to date not widely implemented.[19] Applying the law to the facts of electronic communications — knowing how much impact is needed to make a real and substantial connection with a court's territory — is harder. The topic is a live one, in Canada and in many other countries.[20]

Through online dispute resolution

Not only is resolving disputes through the courts often very slow, but the increasingly international character of electronic communications increases the strength of the case for using alternative means of resolving disputes. Online Dispute Resolution (ODR) is coming into its own, at least in principle. In general, dispute resolution is offered in a wide range of forms and with many techniques, but they come down to two: either the process definitively resolves the dispute for the parties (arbitration), or it encourages the parties to come to their own resolution (mediation). A broader concept extends to techniques of avoiding disputes in the first place.[21] While dispute resolution services are generally private rather than governmental, governments have supported the use of alternative dispute resolution practices both by legislation[22] and by other methods.[23] Dispute resolution is seen as a continuum, from courts through administrative or quasi-judicial tribunals (often specialists in their subject matter) to the full range of private techniques.

A number of commercial and not-for-profit organizations are offering their services for ODR these days.

Consumers International did a study of the criteria by which one would judge such services, at least from the point of view of consumers, and evaluated over 30 organizations according to these criteria.[24] The criteria suggested were availability, affordability, impartiality, transparency, effectiveness, liability (legal due process, recognition of statutory rights at play) and oversight. Its conclusions were that "consumers at present cannot and should not trust that alternative dispute resolution systems available online can offer adequate redress".[25] In December 2000, The Hague Conference on Private International Law, the International Chamber of Commerce (ICC) and the Organization for Economic Cooperation and Development (OECD) held a seminar on ODR, which canvassed a number of the outstanding issues.[26] The number of sources of information is increasing rapidly.[27]

Closer to home, the American Bar Association constituted a task force on electronic commerce and alternative dispute resolution.[28] It held hearings in the United States and Europe and published a draft report of the key issues and recommendations, scheduled for consideration at the August 2002 annual meeting of the ABA.[29]

The best known operating example of ODR is the World Intellectual Property Organization (WIPO)'s Uniform Dispute Resolution Procedure (UDRP), which resolves disputes over Internet domain names.[30] This works through a roster of arbitrators from around the world, selected for their familiarity with the Internet and electronic commerce. The UDRP is not an exclusive recourse, and disputants are still able to take domain name disputes to the courts. The exact boundary between the contractual recourse to the UDRP and the compulsory jurisdiction of the courts remains to be developed fully. Courts were slow to recognize the legitimacy of alternative dispute resolution offline.[31] It is likely that an accommodation will be reached more quickly for ODR.

In any event, governments find the process of interest. The negotiating draft text of the Free Trade Agreement of the Americas published in July 2001 provided that all domain name disputes among participating countries should be submitted to the UDRP.[32] Meanwhile, the Canadian Internet Registration Authority (CIRA), which manages the *.ca* top level domain, has set up its own dispute resolution policy for domain names, modelled after the UDRP and offered online.[33]

Civil regulation

Of more direct concern to governments than the resolution of private disputes is the exercise of regulatory control, where governments have made rules for private conduct that they want to see obeyed. Electronic and borderless communications pose several challenges to such civil regulation. First, unregulated enterprises can readily "enter" the territory electronically to solicit business, for example, by electronic mail. Second, consumers, or other groups that the rules are designed to protect, may deliberately or unwittingly deal with enterprises who are beyond the control of the consumers' governments and possibly not subject to their rules. Third, many services and intangible goods (software and recorded music being common examples) can be provided through electronic media, and payments made online, so no physical contact is needed between merchant and customer at any stage of a transaction.

The legal response to these challenges is less well developed than that to the jurisdiction of the civil courts.[34] A number of attempts are being made, however, some based on law and some on education or private self-help.

Administrative law responses

Four Canadian regulatory tribunal decisions have attacked the issue directly.

The Canadian Radio-Television Commission

The first is the decision of the Canadian Radio-Television and Telecommunications Commission (CRTC) on regulating the Internet itself.[35] The CRTC decided that it had the legal power to regulate the Internet, because material that was not alphanumeric text or customizable for individual users fell within the definition of "broadcasting".[36] However, it also decided not to regulate it at this time, because the public interest did not require it. There were enough sources of information and enough diverse voices, and the ability to provide content on the Internet was sufficiently easy, that the values to be protected by regulation did not need such protection.[37]

It might be noted that the physical infrastructure of the Internet and the market conduct of the participants, be they telephone companies or cable companies or Internet Service Providers (ISPs), are subject to regulation. What is not regulated is the content, though that is subject to the usual criminal laws about obscenity and illegal gaming, for example. Values of free speech would tend to persuade one not to try to impose any regulation on content not applied offline as well.

The Alberta Securities Commission

An important Canadian case which did regulate online activity was the World Stock Exchange decision of the Alberta Securities Commission in 1999.[38] Securities were being sold electronically in Alberta by a company (World Stock Exchange: WSE) registered in the Cayman Islands and operating from a server based in Antigua. The principals of the World Stock Exchange lived in Edmonton, Alberta. The principals of many of the companies listed on the WSE also lived in Alberta.

The Commission found that it had jurisdiction to investigate the sale of securities by the WSE. Not only

were the principals in Alberta, but Albertans were able to trade securities through the WSE. The Commission examined at length the purpose of the regulatory scheme in the *Securities Act*,[39] and found a system by which stock exchanges regulated elsewhere were recognized as legitimate for Alberta purposes. However, unregulated exchanges were subject to direct orders of the Commission. The WSE was not regulated anywhere else, and thus there was a need for regulation to protect Albertans. This fell within the statutory purpose, and justified action by the Commission. There was no place better suited to regulate than Alberta, no other place appeared ready to regulate, and there was some hope of enforcing orders because of the residence of the principals.

The Copyright Board

The other Canadian administrative decision of note in a discussion of civil regulation is that of the Copyright Board in determining a tariff for public performance of musical works online.[40] The Board had to discuss a number of issues that resemble those of other regulatory bodies: when is a communication effected on the Internet? Who effects communications on the Internet? When does the act of authorizing a communication on the Internet occur? When does a communication on the Internet occur in Canada?[41]

The Copyright Board decided that music is not performed when made available on a server, but only when it is communicated in response to a request. The person who puts information on a server communicates it when it is pulled from the server and that person is responsible for its communication. Internet intermediaries, such as Internet service providers, do not communicate the work. Communication occurs at the site of the server where the music is stored, wherever the request came from or the location of the original Web site. Thus the tariff could apply only to servers located in Canada to which content has been posted.[42] The decision was appealed by several of the parties. The Federal Court of Appeal[43] generally upheld the findings on the liability of intermediaries.

The Board's decision to tie the legal rights to the server was overruled.[44] It must be said that the original holding was unusual. The *United Nations Model Law on Electronic Commerce*,[45] followed by the *Uniform Electronic Commerce Act*[46] and most of the implementing statutes in Canada,[47] provide that an electronic message is sent from the place of business of the sender, and received at the place of business of the recipient.[48] The purpose of this is to focus on the real legal relationships and the places in which the parties to a communication operate, and not on where the server is, which may be an arbitrary place, possibly even unknown to the parties who establish communications or a Web site.[49] It is also arguable that putting the weight of the law on the location of the server makes avoiding the law too easy, since the location of the server in practice makes almost no difference to the quality of the communications or the facility with which a content provider can use the service or operate on the Internet. Moving the server out of the jurisdiction, or leasing space on a foreign server, is therefore often not difficult at all. The presence of the server could even be argued not to be a "real and substantial connection" with a particular territory for the purposes of establishing jurisdiction of a court in private disputes. The Federal Court of Appeal focussed on the real and substantial connection in overturning the Board's decision.[50]

That this decision dealt with copyright is significant in itself. One of the main tools for regulating content on the Internet is the enforcement of intellectual property rights. Allegations of copyright infringement have been used to banish from the Internet material that the copyright holders did not want published for other reasons.[51] Copyright law was used by broadcasters and program producers to chase their webcaster competitor iCraveTV off the Internet, allowing time for the traditional industries to figure out how to profit from the new medium.[52] "Business process patents" have been used, particularly in the United States but potentially in Canada as well,[53] to control competition. As noted earlier, the international enforceability of intellectual property rights is one of the key points on which the debate turned with respect to the proposed Hague Convention on the Recognition and Enforcement of Judgments.[54] Intellectual property is protected only because of government action, i.e., legislation,[55] and government can use the nature and scope of intellectual property to help channel behaviour in electronic communications.[56] Developing this argument would take us beyond the scope of the present article.[57]

The Canadian Human Rights Tribunal

The Canadian Human Rights Tribunal decided in early 2002 that hate literature appearing on a Web site based in the United States was nevertheless capable of constituting material disseminated by use of telephonic communications within the authority of the government of Canada, and therefore that it could make an order to remedy this activity.[58] The Tribunal found that the overwhelming majority of Internet communications were carried by telephone, despite the existence of alternatives like cable or satellite, and that the use of the phone network was the key, not the type of device used to connect to it.[59] The Tribunal ordered the respondent to stop disseminating the offensive material on the site. As the respondent has apparently ceased to reside in Canada, the enforcement of the order may prove problematic. The Tribunal recently ordered offensive parts of another Web site removed from the site, finding once again that postings on a Web site constituted telecommunications for the purpose of the Tribunal's enabling statute.[60]

Consumer protection

One of the major tasks that governments have set themselves in the past few decades is the protection of the consumer against improper business practices. Consumer protection statutes have become commonplace, either general in scope[61] or aimed at particular areas of mischief.[62] Business-to-consumer electronic commerce presents a paradigm case of the difficulties described earlier of knowing who is doing what with whom.[63] How do the established consumer protection rules apply online? Governments have chosen a range of ways to respond to these difficulties.

Canada

The consumer protection laws in Canada are not uniform, though the general approach to most issues is consistent.[64] This presents a number of challenges for a harmonized approach to applying or extending protection in electronic commerce.[65] Canada's approach in practice to protecting consumers on the Internet has been to push for information, so that consumers can make their own decisions. A working group representing business, consumers and governments developed guidelines for proper conduct in Internet consumer commerce which emphasized disclosure of information about where the merchant was and what rules governed the transaction.[66] The guidelines do not address the merchant's problem in knowing where the consumer is, though opportunities for fraud on the consumer's part also exist. Presumably, the scale of the problem is not so large as those caused by the inaccessible merchant. If a consumer buys hard goods they must be delivered, allowing the consumer to be traced or the relevant jurisdiction identified before delivery. If a consumer pays by credit card, then the payment is fairly safe for the merchant wherever the consumer is, though there are some risks for the merchant as well in remote transactions. For a consumer to get recourse against an unknown merchant is still harder.

In the spring of 2001, the disclosure principle formed the basis of a template for legislation by the provinces and territories to protect consumers in Internet transactions.[67] The work has been built to a large extent on existing directives about "direct selling".[68] The template requires that all the essential terms of a contract be available to the consumer before the transaction is made, and then that the contract itself be delivered after it is made.[69] The consumer is allowed to rescind contracts made where the merchant does not comply with the rules.[70] In addition, if the transaction has been paid for by credit card, the consumer is given rights to have the credit card issuer reverse charges where the merchant has not complied with the rules.[71]

Manitoba enacted consumer protection rules as part of its electronic commerce legislation in 2000.[72] The rules are much like those in the template, including the rights against credit card issuers. Alberta has by regulation made the template, which it played a major role in developing, part of its law.[73]

The template does not deal with the jurisdiction question directly; the text does not say to what transactions it applies.[74] Further work is underway on that topic.[75] In sum, the governments have, to date, made law on what is to be disclosed and provided a private remedy for not disclosing it. They leave to the courts the task of deciding when the private remedy will be available, pending a legislative solution.

One should note a particular kind of consumer protection regulation: French language rules in Quebec. Quebec has legislation requiring that enterprises transact business with the public predominantly in French, and that advertising for these enterprises should be predominantly French as well.[76] The Office of the French Language has stated that this extends to Web sites of businesses with an address in Quebec, where products are available to consumers in Quebec, wherever the server is located.[77] It does not purport to apply Quebec law to enterprises with no physical presence in the province. The Office has engaged over the years in some correspondence with Quebec businesses that it thought had too much English on their Web sites. It has recently won a couple of prosecutions, in the Quebec Provincial Court, in support of its claims of jurisdiction.[78]

United States

The United States has taken a different tack, nationally. Its federal legislation authorizing the use of electronic documents and electronic signatures, the *Electronic Signatures in Global and National Commerce Act*,[79] known as E-SIGN, expressly excludes or limits its application to consumer transactions. The Act is particularly concerned with "post-transaction" and "post-default" notices, where the consumer may suffer adverse consequences for failure to receive or to reply to the communication. In other cases, E-SIGN requires clear evidence that the consumer is capable of communicating electronically with the merchant, for example by confirming the contract through the same communications channel to be used for later communications.[80] An early evaluation of how these provisions were working was inconclusive, but participants wanted the legislation left in place rather than being amended before people learned to live with it.[81]

Proposed U.S. federal "interim final" rules pursuant to this Act have been published by the Federal Reserve Board for financial transactions.[82] According to the Board, its rules constitute,

> … uniform standards for the electronic delivery of federally mandated disclosures under five consumer protection regulations: B (Equal Credit Opportunity), E (Electronic Fund Transfers), M (Consumer Leasing), Z (Truth in Lending), and DD (Truth in Savings).
>
> Under the rules, financial institutions, creditors, lessors, and others may deliver disclosures electronically if they

> obtain consumers' consent in accordance with the requirements of the Electronic Signatures in Global and National Commerce Act (the "E-Sign Act"), enacted in June 2000. The Board's interim rules provide guidance on the timing and delivery of electronic disclosures, consistent with proposed rules issued by the Board in August 1999, to ensure consumers have adequate opportunity to access and retain the information.[83]

In short, U.S. federal action rests on a combination of limiting consumer transactions in electronic commerce, and requiring disclosure of the kinds provided in Canada as well. The Federal Reserve Board is responsible for monitoring compliance with its rules, and has a range of sanctions available for non-compliance. In short, so long as an offending institution is within its reach, the electronic medium of the communications does not matter. Once the communications are coming from abroad, there is a problem.

The debate continues in the United States about how many consumer-protection limits should be built into state legislation to implement the *Uniform Electronic Transactions Act*,[84] which itself does not have consumer protection provisions, except arguably the rescission right for mistakes in dealing with electronic agents.[85]

The European Union

The European Union has published reports on consumer protection in electronic commerce. The general distance selling directive of 1997 resembles the proposals for Canadian law.[86] The best known proposed rule would ensure that any consumer could have his or her own domestic law apply to an electronic financial transaction, and a dispute could be brought in his or her own court. Merchants in Europe have expressed concern about this, as it exposes them to 15 different legal regimes in their own market.[87] Recently, the European Commission proposed a two-tier rule, with Internet transactions subject to a different rule from offline transactions.[88] The issue is more open than it appeared to be, and its resolution less certain.

The EU has also been active in promoting cross-border administrative and judicial assistance to consumers. The Directive on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market[89] makes basic provision for such cooperation.[90] It also allows states to restrict inflow of consumer-oriented information if the state considers the information to be harmful and the originating state does not take adequate measures to remedy the problem.[91]

A recent study in Canada has proposed a comprehensive approach to governing consumer protection, taking some inspiration from the EU approaches.[92] The study reviews provincial and federal competence in the field and the extraterritorial powers of both levels of government. In a nutshell, it recommends that there be a presumption in favour of the applicability of the prescriptive rules of the consumer's residence. However, mutual assistance measures would assist out-of-jurisdiction enforcement, since enforcement is likely to be most effective in the vendor's place of business. (Making the contracts unenforceable against the consumer at home, as the template does, is some help too, but that technique will not always provide an effective remedy, depending on the nature of the complaint.) Finally, the principles of consumer protection as they apply to e-commerce should be harmonized as much as possible, even if domestic rules remain diverse. Such harmonization would promote interjurisdictional enforcement.[93]

Privacy protection

A very prominent element of the civil regulation of online activity is the legislation being enacted or proposed throughout the world to impose privacy standards on the creators of databases. The privacy discussion is beyond the scope of this article, but business-to-consumer electronic commerce has multiplied the opportunities for collecting personal information, and business-to-business electronic commerce has done the same for opportunities to use and share it. The social need for privacy protection existed before computers, and the use of computerized databases presents challenges for privacy even if the information is collected offline.[94]

The wide degree of uniformity of principles for protecting personal information[95] and the universality of the concern about it give this field of government regulation of the Internet a better chance of succeeding than many. The well-known European Union directive on privacy[96] aims squarely at the interjurisdictional transfers of personal information by prohibiting enterprises within the control of member countries from transferring such information outside their borders without assurances of its adequate protection at its destination.[97] Nevertheless, such efforts must contend with the technology of communications, which allow enterprises outside Europe to deal directly with, and thus collect personal information directly from, individuals within Europe without detection by European officials. Enforcement is partial at best.

Alternatives to direct regulation

Given the difficulties mentioned to this point in direct government regulation of activities on the Internet or otherwise conducted by electronic communications, less direct methods of control or management are being attempted. Some of them are led by government, some of them are substitutes for government. The latter take us beyond the scope of the present inquiry, but deserve a mention here in passing.

Alternative control points

Where government has little control over the entities conducting the activity to be regulated, it sometimes seeks out other elements of the electronic communica-

tions network which are more accessible or amenable to pressure. Much electronic commerce on the Internet depends on the availability of payment mechanisms, and one of the most common is the credit card. Credit cards have dealt with remote transactions for years; the expression "MOTO" (mail order/telephone order) is an industry norm.[98] The issuers of credit cards have contractual relationships with cardholders and with all the merchants in the system. Governments can put pressure on this system to achieve their policy results. The best example on the civil side is the one noted above in consumer protection legislation, where card issuers are required to reverse transactions and charge back sums paid to merchants if the merchants do not comply with their obligations under the legislation.[99] The merchants may be out of the jurisdiction, but some card issuers are usually inside it.[100] Consumers would come to know which issuers are subject to local chargeback legislation and can choose this advantage in dealing with them.

Another control point susceptible to local control is the provider of access to the Internet. Internet Service Providers (ISPs) may be made responsible for the content of communications passing along their facilities, either as publishers of the information flowing through or as hosts of information that their clients put on their servers. The usual civil example is liability for defamation, where the traditional defence of innocent dissemination did not apply, at least in England.[101] ISPs have been the focus of attempts to enforce copyright as well; copyright holders have begun to demand that ISPs close down infringing sites or block them.[102]

In Canada, only Quebec has legislated directly on ISP liability.[103] The Tariff 22 decision by the Copyright Board, upheld by the Federal Court of Appeal, decided that ISPs were not responsible for retransmitting infringing copyrighted material.[104] The United States excluded civil claims against ISPs in many instances in 1996.[105] A court held recently in the United Kingdom that ISPs would not violate a court publication ban if they merely served as a conduit for information communicated contrary to the ban.[106] The European Union's Directive on Electronic Commerce exempts ISPs from liability for content they merely convey without hosting.[107] How far ISPs will ultimately be exposed to enforcement actions is still uncertain.

A third control point concerns industries related to electronic communications that are already regulated. The CRTC has ordered that cable television companies must provide discounted service to competing Internet Service Providers.[108] In the United States, efforts are also being made to ensure that cable television companies do not take advantage of their ownership of wires going into many homes to capture the market in high-speed Internet connections. This is alleged to compete unfairly with other access providers. The matter has been litigated in Oregon[109] and elsewhere,[110] and the subject of federal regulatory action by the Federal Communications Commission.[111] It appears therefore that the use of alternative control points may prove a fruitful regulatory technique.

Technological controls

One of the challenges faced by civil regulation is that it is hard to know where someone is on the Internet. This seems to be changing through the development of more accurate technology for locating computers. This allows people sending messages to target their audiences in particular places. Internet broadcasters may be able to restrict the reception of their signals to places where copyright law or broadcasting law allows such retransmissions.[112] Merchants may be able to prevent their messages from being read in places where local law does not allow them.[113] This, in turn, allows governments and courts to find that messages available in particular jurisdictions were intended to be there and not everywhere in the world, so regulatory powers may be exercised with more confidence.[114] Regulation becomes both more possible and more fair.[115] However, no blessing is unmixed: privacy advocates are concerned about the ability of the same technology to track the whereabouts of individuals.[116]

Another use of technology to enforce legal rights that might escape traditional enforcement, and thus undermine governmental policy, is that which allows copyright owners to prevent copying or performance of their works without compensation. Encryption or special coding, sometimes under the name of "trusted systems", can inhibit the copying or performance of texts and music. Some manufacturers make CD-ROMs in a way that they cannot be copied without interfering with the quality of the sound, to prevent pirating.[117] Unlicensed copies of software can be made to destroy themselves after a period. This is becoming common for software sent on approval or for testing; after the test period runs out, the software stops working.

However, the technology does not always work for long, given the temptations to break protective codes. Stephen King published an electronic novella in 2000, but the code that permitted only paying readers to have access to the text was quickly broken.[118] Copy protection methods designed by the recording industry were put out as a test to code-breakers in 2000, and several people claimed to have broken them.[119] The United States has passed legislation prohibiting the publication of information on how to break security codes,[120] in order to support the use of technology to protect intellectual property.

Efforts to use technology to distinguish permitted from improper copying have not yet succeeded. Napster, the digital music sharing company, was recently told by a court that its efforts to block files which it did not have the right to share had to work all of the time or its service was illegal.[121] The attempt to create an "audio

fingerprint" of music to be banned has run into technical and legal problems. Earlier efforts to block copyrighted music by reference to its title were readily avoided by changing the titles.

In the United States, the original version of the *Uniform Computer Information Transactions Act* (UCITA)[122] expressly permitted licensors of information to use such "self-help" features to enforce their rights. However, the technique was roundly criticized, notably for failing to accommodate the existing statutory balance of paid and free uses of copyrighted material at law. An absolute bar to unpaid use gave the owners of copyright more power than the legislature had given them.[123] As a consequence of these criticisms, UCITA was amended in 2000 to restrict the self-help provisions.[124]

The topic of digital self-enforcement has become very heated in the past year or two. The Canadian government has it under study, in the light of a Supreme Court of Canada decision saying that copyright law has to balance the interests of creators and users.[125] The European Union has also published its thoughts on the topic.[126]

Education

Governments also respond to the difficulty of regulating civil activity by attempting to educate the people whom it seeks to protect. The Principles of Consumer Protection for E-Commerce have already been mentioned.[127] The Principles documents include "best practices" both for consumers and for merchants that want to create trust.[128] The American Bar Association has a similar education site, called *Safeshopping.org*.[129] Securities regulators have also invested heavily in educating investors, so that the investors will be cautious about information about securities that they find online.[130] This is a natural supplement to their general education provisions, such as the "game" on the Ontario Securities Commission's site called "Spot the Bull".[131] Offices of consumer protection also engage in straight education; the Federal Trade Commission is very active in this field.[132]

Virtual communities[133]

As noted, one of the challenges to government's power to regulate activity on the Internet is that people can "go" where they want and get information from, or do transactions with, whomever they wish. Neither the citizen nor the merchant pass through any government checkpoint. The ability of the user to decide where to go, however, includes an ability to decide to go only to safe places. Some governments have considered going beyond education to establishing such safe places themselves. Here we are not talking about places for dealing with government services, which were discussed under electronic service delivery. The picture here is of a "place" on the Internet where merchants are voluntarily regulated, because their being regulated makes people feel safe in dealing with them and thus increases their business. If the government was generally regarded as an honest and competent regulator, then having its regulatory supervision would be an asset.

Those who submit to regulation must in some way be subject to traditional means of enforcement by the regulators. Where governments regulate, the obvious candidates for regulation are those who are physically in the regulating jurisdiction. Others might post bonds or give other security for good behaviour. Such a system was proposed to the Ontario Ministry of Consumer and Business Services (as it now is) by Professor Michael Geist early in 2000.[134] The economic advantage to the regulating jurisdiction was hypothesized by Professor David Post in the context of Internet gaming: a place that could guarantee honest games and effective payout of winnings would attract the technology jobs and cash flow of online casinos.[135]

Not only governments seek to provide these safe environments. In fact, the private sector got there first. Both the merchants and the supporting organizations are working to make this model of safe communities work. America Online (AOL) guarantees satisfactory online shopping with merchants on its site; if efforts to resolve disputes directly with the merchants fail, AOL will ensure the customer is satisfied.[136] No doubt AOL has some clout with the merchants to ensure that AOL itself is rarely out of pocket. Its contracts with the merchants give it the power to enforce that a government might lack. Likewise, the online auction site eBay offers its "Safe Harbor" services, which among other things provides its users with insurance against fraud[137] and offers them a third-party dispute resolution facility, Square Trade.[138]

Neutral service organizations also offer guarantees to give comfort to consumers. The Better Business Bureau has extended its traditional services to online transactions.[139] Chartered Accountants in Canada, working in concert with Certified Public Accountants in the United States, have created the "WebTrust" program to accredit the honest business practices and the security systems of sites that are given permission to post the "seal" of the program.[140] The most active area of such private certification services is the review of privacy policies. Both services mentioned will certify the practices of the Web site in collecting and using personal information. Another significant source of such accreditation is Trust.e, a private non-profit organization.[141] Naturally, certificates or seals of approval from these groups need themselves to earn the trust of consumers by clear and acceptable principles and a credible examination and audit practice. They do not begin with the level of trust that a government can provide, though not all governments earn equal confidence of the public.

We see developing here a new combination of private and public government of the Internet that helps

avoid the borderless nature of the communications and that builds on the voluntary participation of its users. Widespread concerns about security and privacy on the Internet are likely to make people receptive to such initiatives. The availability of certification programs is likely to prevent the Internet from becoming an unreliable marketplace, where unscrupulous merchants seek out the most lax governing regimes that compete for their presence in a "race to the bottom". Most consumers will not follow merchants in such a race.[142]

Standards

Electronic communications are obviously the products of technology, and technology is not an accident. If it works, and especially if it works consistently over time and space, it conforms to standards of design, construction and operation that permit such working. These standards can control the behaviour of the users of electronic communication. They can be used consciously to do so, or they can do so even if the creators of the standards were focusing more on technological capacity than on regulatory aims. The use of standards is developed in more detail in the final section of this paper, under the heading Cyberlaw, with special attention to the "hidden" regulatory power of standards.[143] It is worth noting here as well, for the sake of completeness, their potential as an alternative to direct regulation of the social or legal conduct one wants to regulate.

Controlling criminal and other offensive behaviour

Besides providing a means for private citizens to resolve their disputes, and regulating commercial and other behaviour in the marketplace, governments have traditionally been in the business of keeping the peace. Preventing, prosecuting and punishing illegal conduct is a hallmark of government activity.[144] Criminal law was to some extent the transformation of disputes about harmful behaviour between individuals into disputes with the Crown instead. Electronic communications presents some new challenges for the government in criminal law and in controlling offensive behaviour generally at the borders of the criminal.

Criminal conduct

The most obvious category of novelty is crimes against computers. Using computers for traditional criminal activity is not much of a challenge in principle: fraud is fraud, whatever the medium. The only challenges come in that field when the language of the applicable statute is phrased to require some more tangible medium for the crime than electronic data. The larger challenge is crimes that affect our increasingly computerized world. Canada moved to ban much activity of this kind in the early 1990s, when a number of offences about unauthorized use of or access to computer systems were created.[145] Many countries have been paying close attention to this, especially when laws are shown publicly to be inadequate by the acquittal of someone that people think should be guilty.[146] Studies are available comparing countries around the world for the adequacy of their criminal laws in this field.[147] Australia is among the most recent countries to adopt a new statute to address this issue.[148]

In addition, prosecutorial procedure may have to be adapted. This presents issues of evidence[149] and of the use of electronic communications to do the police and prosecution work itself.[150] The ability of police forces to detect computer-based crimes is a related issue, and many places have created specialized teams with dedicated resources to develop the expertise required.

Criminal prosecutors face the same problem as their civil regulator counterparts: where the criminals are in the world; is the activity criminal where they are; and who is dealing with them from within the prosecutors' territory.[151] In general, because criminal liability can mean going to jail, criminal law is enforced carefully, with strict limits on procedures and scope. However, some mildly extraterritorial legislation is already in the Canadian statutes, notably imposing liability on people who misconduct themselves on airplanes or commit sexual offences with children abroad.[152] Similar challenges occur on the Internet, with particular weight on cases of fraud and illegal gambling. To date, Canada has not legislated on this point.

The high-water point of asserting criminal jurisdiction in North America remains the Minnesota Court of Appeal's decision in the United States in the *Granite Gates* case.[153] The Attorney General of Minnesota prosecuted the defendant, which ran a legal gambling operation in Nevada, because some residents of Minnesota gambled on the defendant's Web site. The Court held that the defendant knew that people in Minnesota would be attracted to the site, though gaming in general was illegal in Minnesota. Thus, the defendant in Nevada was guilty of violating Minnesota law.[154]

A recent Canadian case came at the issue from the other side. The Earth Fund, an environmental charity, proposed to run a lottery on the Internet, from offices based in Prince Edward Island. The PEI Court of Appeal was asked if the province had the right under the *Criminal Code*[155] to license such a lottery. The Court held that the licence provisions of the Code did not apply, because the use of the Internet meant that the lottery was not conducted, managed or operated in the province.[156] The Court so held despite efforts of the Earth Fund to have all sales deemed to take place in the province and subject to provincial law:[157] "A transaction for criminal law purposes may occur simultaneously in more than one place or jurisdiction".[158] It is not clear if this principle would support the right of another province to prosecute an out-of-province (or out-of-country)

online lottery on the basis that the relevant transaction occurred in the prosecuting province.

Other governments have sought alternative control points. Since criminal liability requires a criminal state of mind, it is hard to convict an intermediary, like an ISP, of the offence. Regulatory pressure is needed. The host of a Web site or the operator of a portal — someone responsible for the content or able to control it — is different, as we have seen. The most notorious example is the *Yahoo!* case,[159] where the large American portal was convicted in France under French law of offering Nazi memorabilia for sale. Controversy has been technical — could Yahoo effectively block selected offerings of its members from selected countries?[160] — and political — should someone communicating in one country be subject to censorship based on another country's laws or customs?[161] One encounters similar issues to those in civil jurisdiction discussions, about active or passive presence in the prosecuting country, targeting, and the like. One also needs to distinguish liability in the prosecuting country and enforceability of that country's sanctions elsewhere. There has never been an international regime for collecting foreign fines, and even extradition of criminals is subject to limits.[162]

Criminal enforcement authorities have discovered the credit card issuer, as have the consumer protection authorities.[163] Federal legislation in the United States has proposed prohibiting credit card companies from paying gambling debts, with the intent of drying up the sources of funds to gaming sites.[164]

Where criminals are located in different countries, it is open to authorities to cooperate to find them. The details of criminal law are not harmonized across the world, but the basics of honest commercial behaviour do not vary greatly.[165] The Federal Trade Commission in the United States has organized an extensive network of governmental authorities to seek out fraud on the Internet, leaving the disposition of what is found to the government responsible for a particular territory to follow up on offenders located in that territory.[166] Canadian government agencies have participated in these international operations, notably the Ministry of Consumer and Business Services and the Ontario Securities Commission.[167] Australia has been actively considering these issues and participating in the international activities, too.[168]

Besides international cooperation, international law reform is in prospect. The Council of Europe, of which Canada and the United States are members, worked for several years recently on a treaty on enforcing criminal laws in the computer field. The Cybercrime Treaty is now in final form, and it has been signed by a number of states, though not yet in force.[169] Some concerns have been expressed that this convention gives excessive powers to the police to oversee computer communications, at the expense of privacy and possibly the presumption of innocence.[170] Canadian proposals to implement the Convention have recently been published[171] and seem subject to similar concerns.

As with civil regulation, so with the prevention of crime, there is private sector activity as well. Merchants group together to create a safe and cybercrime-free community.[172]

Offensive content

Besides criminal activity, governments try to protect their citizens from some kinds of offensive behaviour or offensive displays. Some kinds of offensive information is itself criminal, of course, like hate literature.[173] A draft protocol to the Convention on Cybercrime to criminalize racist speech[174] is subject to considerable criticism as well, on grounds of free expression. Whether or not it is criminal, governments may take steps to prevent its coming to the attention of the citizens.

As with civil regulation, technology can provide some solutions. The nature of Internet communications allows incoming information to be screened or filtered before it is displayed on the computer screen. Many services are available to screen content to eliminate what may be thought offensive, based either on the origin of messages from known offensive sites or on the use of selected key words that are thought to indicate offensive content.[175]

Have governments some responsibility to screen offensive content out of government-sponsored computers? Arguments have been made in the positive, based on the need to protect minors and on the desirability of preventing either workplace harassment through display of inappropriate words and images, or a "poisoned atmosphere" of prejudice, mockery or contempt. Negative arguments turn either on the value of free speech, which includes access to information, or on the clumsiness of the filters.

In the United States, the use of filters by a public library was challenged in court by a civil liberties organization.[176] The court held that filtering was unconstitutional as violating free speech.[177] Federal legislation in the U.S. now requires that all libraries that receive federal funding and that give public access to the Internet must use filters to prevent minors from seeing offensive content.[178] This legislation was successfully challenged on constitutional grounds.[179] In Canada, no such legislation is planned. However, it is common for institutions to install filters; the government of Ontario network is filtered so its public servants cannot visit inappropriate Web sites.

The other notoriously offensive content on the Internet is unsolicited commercial messages, known as spam. Spam is harmful because it is a nuisance and it imposes a cost on Internet users and particularly on ISPs in bandwidth consumed for what are usually unwanted messages. Those who pay for linkage time to the Internet

incur a cost merely in downloading the spam from their e-mail servers in order to delete it.

The Canadian government, through the CRTC, decided in 2000 not to regulate spam, at least at this time.[180] It was thought that a combination of technology (filters[181]) and contractual prohibitions by ISPs would suffice to keep the nuisance level low.[182] Elsewhere, stronger legal tools have been sought. State legislation against spam in the United States has often been struck down as a violation of free speech or as improper restrictions on interstate commerce,[183] but Washington state courts have upheld that state's version.[184] Federal bills are constantly before Congress on the subject, though none has yet passed.[185] Recently, the European Union has adopted a Directive to regulate spam as well, choosing an opt-in approach (requiring the addressee's consent to receive the message), though a committee of the European Parliament took the view that spam is a legitimate business practice.[186] If spam were banned, the committee reasoned, then others than Europeans would profit from it regardless of the ban, but Internet users would not see a reduction in the amount of spam they receive.[187]

Summing up on jurisdiction

The question of jurisdiction in electronic commerce and regulatory matters has been debated since the Internet started to become very popular, after the creation of the World Wide Web in the early 1990s. The legal responses available for government to ensure that it can do its job — resolve disputes, control commercial behaviour, fight crime and block offensive information — have been developing more recently. The field is very much in evolution, as is the balance between technology and legislation as the preferred tools for control. One of the longstanding responses to problems of jurisdiction is harmonization of laws; if the legal rules are the same, then the choice of law and, to some extent, of forum are less important. We have looked briefly at the harmonization of consumer protection rules earlier.[188] We look at harmonized standards in the final part of this article.[189] In addition, the private sector forms a number of intersecting Internet communities, whose practices and sensitivities are also evolving rapidly. To the extent that such community standards are important to the legitimacy of government regulation and to the definitions of crime, the task of e-government becomes more uncertain. We see outlines of solutions in the mist, but the details may turn out to be different from how they appear at present.

The Electronic Economy

Governments have traditionally been responsible for the currency, to guarantee its soundness. The ruler's portrait has been on coins for millennia, as a symbol of that guarantee. In the past century, the role of government in regulating the economy generally has substantially increased. The principal tools for fulfilling that role are monetary and fiscal policy: the control of the money supply and the imposition of or granting relief from taxation. The electronic economy challenges the use of both of these tools.

Electronic money

Money is a store of value, i.e., a way of keeping wealth, and a medium of exchange, i.e., a way of measuring the worth of goods or services being transferred. Over the years, money has been turning into a form of information. Most people do not hold significant amounts of currency, they have accounts in financial institutions that represent debt to the depositor; they have an account receivable with the bank. The wealth is not in its holders' vaults, it is on their books. The same is largely true of other forms of investments. Likewise, payments are made by changing the information to represent increased value in the name of the payee and less value in the name of the payor.

This trend is accentuated with electronic money, digitized information. Financial institutions have kept their clients' money — their accounts of information — on computers for years. Much more recently, means have been made available to individuals to use money in electronic form. The principal manifestations of electronic money have been smart cards containing a microprocessor to store and amend the information about the value stored or transferred. Some cards are stored-value cards, which contain information representing a fixed value, downloaded from a financial institution. When the money is spent, the value is transferred to the payee and the card holds less value, down to the time when it needs to be refilled. Other cards are access cards, which enable the cardholders to access their accounts to draw out money directly. This is equivalent to a debit card.[190] The older variant of this is, of course, the credit card, which allowed a deferred transfer of value from the cardholder to the payee.

Credit cards and debit cards are well recognized, and the former at least are the foundation of most business-to-consumer electronic transactions. The use of a card that itself contains the value transferred in a transaction that would otherwise be done in cash is less widely accepted. Recent trials of stored-value cards in Canada have not been successful. Mondex, one of the main purveyors of such cards, has deferred its expansion of the technology due to the indifference of many of its proposed customers.[191] The future may be to combine the e-cash function with other functions, like that of a debit card. This was done in the pilot project in Sherbrooke, Quebec.[192] The French system, Moneo, the product of a broad collaboration among banks and communications companies, appears to be spreading more regularly.[193] Demand for electronic payment has been stimulated by passage to the euro as of January 2002.

While electronic cards may be usable for payments, the questions for government are whether they are part

of the money supply to be regulated, and if so, how to regulate them. A strong argument can be made that stored value cards of the kind issued by Mondex Canada are money in a legal sense, though not currency or legal tender.[194] This conclusion depends on there being fairly wide acceptance of the cards as a payment mechanism, which, in the light of the discontinuation of the pilot projects, appears premature. Government discharges its role as regulator of the money supply partly by issuing or not issuing new currency, and partly by credit policies that stimulate or reduce demand for money. Neither method is likely to be affected significantly by electronic money in the foreseeable future. More widely used electronic alternatives to currency will have more impact, more for the difficulty of detecting and measuring them than for their legal characteristics.[195] However, the records of major payment system participants, notably the banks, are available to government regulators and statisticians, so the global impact of electronic transfers is likely to be detectable for some time.

Legal tender is money that a creditor must take in satisfaction of a debt. Singapore has announced that it will make electronic money legal tender in that country by 2008, using a combination of smart cards and wireless equipment.[196] No legislation has been introduced to date to support this development.

Taxation of electronic transactions

Governments depend on tax revenue primarily to pay for their own operations of their programs, and the operations of those that depend on them for funding, and also to spur the economy by fiscal policies. As transactions are conducted electronically, governments face several challenges in maintaining tax policies. The revenue authorities in Canada have been studying the implications,[197] as have experts abroad. The OECD has published a number of other studies of tax consequences of electronic commerce.[198]

One of the hardest problems presented by electronic transactions is knowing that they have taken place at all. This is particularly important for sales or consumption taxes, such as Canada's retail sales taxes[199] or the federal Goods and Services Tax,[200] or value-added taxes in Europe. The more that transactions can be completed online, with no physical delivery of goods to be traced or physical movement of service personnel to monitor, the easier it is for those transactions to escape reporting and thus to escape taxation. To the extent that electronic payment systems are widely available, and value can be held outside the taxing country, the problem is aggravated. Add to that the use of strong encryption, so that electronic messages cannot readily be read even if they could be intercepted, and the difficulty is greater still.[201]

These are practical rather than legal problems for government. The legal requirement to collect and pay tax on a transaction does not change, nor does the obligation to report income and pay tax on it. Some tools have been developed to collect tax on income even where it is not declared. "Anti-avoidance" measures are not new with e-commerce. The federal government has the power to estimate income from circumstantial evidence, in some cases.[202] It has been said that nobody lives in cyberspace. The trappings of wealth are likely to be noticeable, but hoping to notice such evidence or waiting for reports of it seem like difficult strategies.

Another problem for taxation of e-transactions is the jurisdiction question raised in detail earlier in this paper. Where is a transaction taxable? A good deal of thought has gone into this.[203] Many countries have tax treaties to avoid double taxation of residents doing business across national borders. The treaties allocate transactions to one jurisdiction or another so they can be taxed. One of the key concepts is that of "permanent establishment", the presence of which for an enterprise attracts taxability. What constitutes a permanent establishment of an online business? The Organization for Economic Cooperation and Development (OECD) has published a study on that topic,[204] which concluded that having a Web site accessible in a country did not give its owner a permanent establishment there. Having a computer server in a country might well constitute a permanent establishment.[205] It was thought, however, that it was so easy to move computer equipment, or to acquire access to equipment elsewhere, that a finding that a server implied a permanent establishment would have few if any unexpected adverse tax consequences for e-businesses.[206] The government of Hong Kong recently came to similar conclusions.[207]

A separate legal issue combines the practical challenge of dematerialization with the technical rules of tax both nationally and internationally. For income tax and consumption tax purposes, transactions depend on their character, for example as services, sale of tangible goods, or transfer of intangibles, among other things. Electronic commerce blurs the distinctions. Consider buying a book at a bookstore and downloading an electronic book from the Internet. Is the latter a transfer of intangibles, or the receipt of a service? Both characterizations are possible for sales tax in Canada, but the European Union characterizes it as a service only. A study paper by the OECD[208] says that such a transaction gives rise to "business profits", without saying whether it relates to the sale of a tangible or intangible. While this does not matter for tax treaty purposes, income tax falls differently on business profits and royalties for the licence of intangibles. Sales taxes fall on the sale of goods but not on the sale of services (except of course for a goods and services tax).[209]

Another issue for governments in dealing with the taxation of electronic commerce arises because they generally want to encourage the move to electronic communications, which are considered more efficient and more competitive than traditional ways of doing business. As a result, many governments have wished to avoid creating

tax burdens on electronic businesses.[210] Not only do they not wish to impose new focussed taxes on the new technologies, but they have often accepted that a no-tax policy will result in transactions going tax-free that would have been taxed if done offline. Besides its unfairness to offline businesses, this is a threat to the revenues of governments that depend heavily on transaction-based taxes. Therefore, as e-commerce becomes less of a novelty, some people may start pushing to remove the moratorium and find a way to tax at least equally with other transactions.[211] This debate continues, in the United States[212] and the European Union.[213]

Institutions of Electronic Government

Electronic Democracy

Electronic communications and information technology protocols extend beyond the delivery of government services and the regulation of economic relations, on a micro- or macro-economic scale. They are beginning to affect how governments relate to the public that elects them and how they perform not their regulatory but their governance function. We will look at three elements of this set of phenomena: public dissemination of laws; the conduct of elections; and government–citizen relations, other than program delivery.[214]

Dissemination of the laws

Every person is presumed to know the law. In a democratic society, the people have a need and a right to have access to the law. Electronic publication makes these statements more readily realizable. Legal texts, whether statutes and regulations or decisions of the courts, can be made available at relatively low expense for both supplier and recipient compared to printing and distributing paper versions, usually in bound books. At present the federal government and most of the provinces make their legislation and regulations available online.[215] Court decisions are less widely available electronically, partly because printing has been in private hands for many of the series of law reports. The private sector is helping. In Canada, the Federation of Law Societies sponsors the Canadian Legal Information Institute which aims to make sources of Canadian law available online for free.[216]

One issue for governments wishing to put their laws on the Internet is whether the electronic texts have official status, or whether for legal purposes one still has to rely on the law as printed on paper. The government of Ontario e-laws site has the following disclaimer: "The data on this Web site is provided as a convenience only and should not be relied on as the authoritative text. The authoritative text is set out in the official volumes and in office consolidations printed by Publications Ontario."[217] The questions to resolve are those of electronic service delivery: authentication and security, but the implications are more fundamental to core values of the state, as making and enforcing law is the essence of state power. To date, therefore, Ontario has not given its electronic legal publications the same status as preferred evidence enjoyed by published law on paper.[218]

The federal government has started the legislative process to give electronic laws their full legal effect. The *Personal Information Protection and Electronic Documents Act*[219] amended three federal statutes in this direction. Amendments to sections 19 through 22 of the *Canada Evidence Act*[220] replace "printed by the Queen's Printer", including the Queen's Printer for a province, with "purported to be published" by the same authority. The person seeking to introduce evidence need not prove who published the documents in electronic form. The security is to be built in by the government so the user does not need to prove more about provenance than may be reasonably expected.

The *Statutory Instruments Act*[221] was revised to permit the Queen's Printer to publish the *Canada Gazette* in electronic form,[222] and to ensure that a version of a statute or regulation published online by the Queen's Printer is deemed to have been published in the *Canada Gazette.*[223]

Finally, once the legislation is proclaimed in force, the *Statute Revision Act*[224] is to be renamed the *Legislation Revision and Consolidation Act.*[225] It provides for regulations to be consolidated from time to time and kept on paper with the Clerk of the Privy Council,[226] as statutes are already under the *Publication of Statutes Act.*[227] The statutes and regulations may be published in electronic form:

> **28.** (1) The Minister may cause the consolidated statutes or consolidated regulations to be published in printed or electronic form, and in any manner and frequency that the Minister considers appropriate.
>
> (2) A publication in an electronic form may differ from a publication in another form to accommodate the needs of the electronic form if the differences do not change the substance of any enactment

Likewise, they may be readily used in evidence:

> **31.** (1) Every copy of a consolidated statute or consolidated regulation published by the Minister under this Act in either print or electronic form is evidence of that statute or regulation and of its contents and every copy purporting to be published by the Minister is deemed to be so published, unless the contrary is shown.

The main security principle is that the printed version of the statutes or regulations deposited with the Clerk of the Privy Council prevails over any electronic version if they are inconsistent.[228] To date, however, the statutes published at the Department of Justice Web site do not purport to be official. A short disclaimer leads to a longer recommendation to refer to the *Canada Gazette.*[229] The legislation is not in force, but prepares the way for the secure system yet to be installed.

As laws and law reports go online,[230] questions arise about their durability in this form. Software and hardware evolve quickly, and older electronic texts stop being readily accessible to newer devices and programs. In addition, citation of judicial decisions and those of administrative tribunals becomes more difficult as electronic texts online do not have page numbers. How does one cite a case in a media-neutral way? Such questions are being explored by lawyers, law librarians, and courts.[231] A uniform system of citation has been devised to make electronic law as accessible as law on paper, and the courts are generally adhering to the system, including by numbering paragraphs of judgments for ease of reference online or on paper.[232]

Government has a duty not just to current law but to history.[233] Archivists preserve the official and unofficial memory of government and people. The electronic age threatens their ability to do this.[234] The evolution of technology requires large expense, and many archives are required to keep "migrating" their records through successive versions of hardware and software to maintain its accessibility.

In addition, the use of security techniques, which are a growing part of electronic service delivery by government, presents a new and serious challenge to archivists. Electronic signatures created by encryption will not be readable in the archives unless the archives keep the key for the signatures. Security policy demanding frequent changes of the key, the general turnover of personnel, and the large number of people who generate records subject to archiving, all make this a nearly impossible task. The National Archives of Canada has adopted a policy not to accept encrypted signatures on archived records.[235] The United States National Archives and Records Administration has gone further and published detailed requirements for dealing with encrypted documents.[236] These electronic signatures must be accompanied by a plain text version, with the result that one will not be able to check the validity of a signature in an archived document the way one can with a handwritten signature. Other techniques must be followed to ensure that electronic signatures are trustworthy.[237]

In sum, the basic functions of government — making laws and keeping records of its actions — become newly challenging in the electronic age. Governments on the inevitable path of becoming e-governments are dealing with the legal consequences of meeting these challenges.

Electronic voting and elections

The most visible public activity related to government that most people participate in is voting. Voting machines are not new, but electronic voting has appeared more recently. The use of machines operated by voters in person does not present radically new issues, though it is necessary for election officials to ensure that the machines accurately record the votes without being able to relate the voter to the vote.[238] What turns mechanics into a legal question of electronic government is the possibility of voting at a distance. The questions are ones of authentication and security. Who is voting, and how do officials know the person is eligible? Can the vote be altered in transmission, or at either end of the communication channel?

To date no formal elections have been held electronically in western democracies, though the State of Arizona ran its Democratic Party primary in 2000 partly by electronic means,[239] and a number of experiments have been conducted in Switzerland.[240] The *Electronic Commerce Act, 2000* of Ontario[241] expressly does not apply to anything done under the elections statutes.[242] However, financial reports on fundraising are submitted to Elections Ontario by electronic means, without specific authority under the *Election Finances Act*.[243] A good deal of thought is being given in some places to electronic elections, which are seen as a way of increasing the proportion of qualified voters who actually vote, by making it more convenient for them to do so.[244]

Pending the day when online voting arrives, a number of other processes in the electoral field are going online. Political parties[245] and lobby groups[246] make their positions known and solicit both help and money. Senator McCain in the United States primary campaign in 2000 raised a great deal of funds over the Internet.[247] The use of online opinion polls is growing,[248] and consultation on draft legislation.[249] An informal opinion poll was developed during the Canadian federal election campaign in November 2000, by which a satirical group asked whether the leader of the Canadian Alliance Party, Stockwell Day, should change his first name to Doris. The site had over a million positive replies in two weeks, triple the number that that party's platform had suggested would be sufficient to compel a government to call a referendum.[250] Countries less comfortable with political satire may see the Internet as one more area of speech to be controlled.[251]

New techniques are developing as well, based on the potential of the medium. During the 2000 presidential campaign in the United States, a movement grew up for "vote trading" across state lines. Vice-President Gore needed to win crucial states to build up Electoral College votes; Ralph Nader needed a certain percentage of votes nationally in order to qualify for subsidies for his party. People offered to vote for Nader in states where Gore would win anyway, in order to build up Nader's percentage, in exchange for votes for Gore where he needed the votes to win the state.[252] There would be no way to enforce such an undertaking, but without Internet technology, the idea could not have been contemplated on a scale needed to be effective.[253] Election officials considered this practice to be equivalent to buying votes, and they moved to close down sites that promoted the practice.[254] The American Civil Liberties Association supported the sites and opposed the closings, on the ground

that this was just a new form of free speech on political topics.[255]

Electronic technology is thus making the old new and creating new where there was no old before. Much of electronic voting so far is talk, but action is not likely to be far behind.

Electronic Governance

The impact of electronic communications extends beyond voting for politicians, into the methods the government uses to govern. This is not limited to electronic administration — business deals between the state and its suppliers.[256] It changes, or has the potential to change, the nature of the relation between the government and the governed. Both politicians and civil servants will be affected. The ability to communicate immediately will lead to expectations that government will be listening. Elites are challenged by the diffusion of information and power. Communications may be one-to-one or many-to-one or one-to-many. As the Internet develops, they will also be many-to-many.[257] New potential and new expectations threaten decision-making processes that assume a controlled consultation process, followed by internal secret deliberations, followed by top-down announcement of decisions, followed by professional implementation.[258]

Opening up the ways government decides, and the ways government gets information, has the potential to affect how we think about representative government.[259] Some political systems have long relied on referendums and plebiscites to allow public opinion to shape government action between elections, or on specific topics at elections. Electronic communications permit mass consultation at little expense, and mass delivery of opinions to government; they work in both directions to lower the barriers to knowing what people want. Expertise may be devalued, and certainly the ability to close the circle of expertise, to claim it for a small group of insiders, will be much diminished.[260]

People wanting to communicate electronically may have little knowledge of or patience for distinctions between levels of government. Originally, much of the division of powers between federal and provincial governments was based on the possibilities of control, as well as on the general impact of federal law compared to the local impact of provincial law. Telephones and air travel have already reduced the power of this logic;[261] the Internet deals it a further blow. Just as governments themselves have to reorganize themselves to provide "one-window" service,[262] to look at themselves "from the outside in, not the inside out", so too they will need to remove barriers between levels.

Another challenge of opening up government is the potential for collecting or disclosing personal information. Computers identify themselves when they communicate, and many people have mail headers in their own names. Information is noted as it is communicated. A balance is needed between keeping the personal information in order to respond to requests or justify demands for service, on the one hand, and ensuring that the personal information is not misused for political or bureaucratic purposes, on the other.

The part of the political system that has most profited from the Internet is arguably non-governmental organizations, because of the power of the Internet to encourage the growth of groups, the many-to-many communications mentioned above.[263] This is particularly true on the international level, perhaps because the formal legal and political structures among nations are weaker than they are nationally, so there is more room for growth and greater likelihood of having one's voice as a novel participant heard.[264] One thinks of the influence of NGOs in international discussions in recent years: against the Multilateral Agreement on Investment from the World Trade Organization; in favour of the International Criminal Court; in favour of strengthening environmental standards at the Rio conference; in favour of a convention to ban land mines; against globalization in Seattle and several other forums.[265] The sharing of information and plans is qualitatively different from what it could be with letter mail, telephone and fax.

Even the traditionally less effective "concerned citizens" are given new arms by the Internet — including the ability to find allies, collaborate, and turn themselves into new NGOs! The Internet "reduces transaction costs", in the law and economics jargon. Communication with a wide variety of people is little more expensive than communicating to a neighbour across the street. New voices can be heard far more readily than they could be when publishing one's ideas meant acquiring a printing press or persuading or paying the owner of a press to provide space.

Finally, the Internet has extended the scope of the participants in public policy debates well beyond one's national borders. Experts and foreign quasi-public organizations have increased their role, by being accessible to law reformers anywhere in the world. One thinks of the more or less passive data banks of law reform projects around the globe, as maintained by the British Columbia Law Institute.[266] The accessibility of experts is greater, however. In many cases, one can just locate an expert's e-mail address and ask! This could be done in writing as well, and still is, but the immediacy and the potential for dialog makes the process more valuable.[267]

Looking at tools of electronic government across national borders, the Internet offers great potential to reduce the economic divide; the infrastructure costs of building an electronic economy, for getting access to the Internet, are lower than those of building other methods of communication. Thus, we see remote or devastated economies betting heavily on the Internet to modernize their nations.[268]

In addition, the Internet is providing to government and citizens the tools of democracy directly in countries that lack them. Much work has been done at the community level in Bosnia and, more recently, in Kosovo to restore political and social links among the people. Dean Henry Perritt speaks of the Internet's ability to "enhance the functioning of state-based and international legal institutions through the Internet".[269] His discussion explores in detail the characteristics of the Internet that suit it to this kind of fundamental law-building. Among them are its decentralized nature, which helps avoid both physical obstacles, whether caused by war or other disasters, and intentional obstacles like attempts to censor it. New kinds of intermediaries will grow, creating a new kind of state in the remains of an old, inefficient, and undemocratic one.

The Internet does not necessarily promote democracy, of course. Methods of avoiding censorship are also methods of avoiding law enforcement and responsibility. Not all revolutionaries have good motives (and not everyone sees "good" in the same way). So, we will have the traditional challenges of ensuring that the right principles prevail, but in a new world of communications and group dynamics. Such novelties will arguably spread more quickly in places where the old communications and social infrastructure is in disarray, rather than in places that are more heavily wired but also more solid in their pre-Internet social, political and economic assumptions.

Summary on e-democracy

Our democratic institutions that make the law and that make it known are affected by new methods of dealing with the public in whose interests the government is supposed to function. These are early days for the Internet in all of these fields. The concerns that permeate government's delivery of online services also affect how the government is chosen and how it organizes itself not just to carry out programs but to function as a decision-making body.

Cyberlaw

The first computers talked to each other in 1969.[270] The Internet was established as a method to link computers in a decentralized way, so that damage to one part of the network would not prevent communication among the undamaged parts. The Internet is not a physical network but a set of rules, or protocols, by which a computer can format and send a set of signals so that other computers can understand it. If one does not follow the protocols, one cannot use the Internet. This is a matter of electrical engineering.

What are those rules, and what assumptions lie behind them? Electronic government as described in this paper relies on computer communications. Both the state and the people have to conform to the protocols, or none of the other attributes will be available to them.[271] Making up the system rules can have consequences for electronic government, for the demands on public bodies and for their ability to respond to the demands, for their ability to govern electronically at all.

The final part of this paper therefore considers some of the arguments about the impact of the technical and political organization of the Internet and how they affect electronic government. They are in a meaningful sense an element of the legal regime to which any electronic government is subject, and thus have a place in a discussion of the law of e-government. We look first at some expressions of the principle of the protocols as law, then at the political structures that govern them, then at the technical organizations that also make decisions affecting the power of governments to be e-governments.

Code as Law

The primary exponent of the principle that computer communication protocols are an important kind of law is Lawrence Lessig, as stated especially in his book, *Code and Other Laws of Cyberspace*.[272] Professor Lessig's thesis is that the protocols have been chosen for particular purposes (such as routing around disaster, as noted above) and by particular people, mostly engineers who put more value on some principles, like free flow of information, than on others, like ability to control the content of information. The value of freedom, however, puts a good deal of responsibility, and a good deal of power, in the hands of participants in the system. If they conform to the protocols, then they can create technology that works to serve those particular participants.

The example often given by Professor Lessig is self-help technology created by copyright owners, already mentioned in this paper.[273] The law has traditionally granted certain limited monopolies in order to give a chance for creators of information to get an economic return from its creation, to encourage them to create it. Thus, statutes grant patents,[274] trade marks,[275] and copyright,[276] and some variants of them.

But these monopolies are limited in time, and they are limited in scope. Particularly copyright, which lasts a long time (life of the author plus 50 years[277]), is limited. Copyrighted information can be used without permission and payment for purposes set out in the statute. In Canada, "fair dealing" is permitted, and some uses without commercial purpose that are not thought to cost the copyright owner dearly.[278] Libraries have some rights, and educators. The scope of these rights has been debated, and methods of compensating authors developed, such as the public lending right for library materials.

Technology can reduce those rights without amending the law. It may be possible to prevent someone from copying an electronic text.[279] This is intended to reduce global piracy, but it means that the

copyright owner, not the statute, decides the limits on the use of its information.

In the United States, at least, there is beginning to be some awareness of and resistance to this kind of technology-assisted law.[280]

More recently, the Librarian of Congress published a rule to implement the anti-contravention provisions laid out in the *Digital Millennium Copyright Act*.[281] They included administrative prohibitions on practices that the Act was intended to discourage, including breaking of anti-copying software (except for finding out what sites filtering programs filtered). This policy has been severely criticized by a number of library and civil liberties groups, and some legislators, on the ground that it lets copyright owners control copying to a greater extent than general copyright policy allows.[282]

Professor Lessig concludes from these and other examples that democratic political controls are needed on the codes used for computer communications. Other commentators put more faith in the market to find ways to preserve freedoms, if monopolies are avoided. They argue that competition will keep the code open better than regulation.[283]

There are policy institutions for the Internet. We now turn to them, to see whether they are institutions of global e-government, or even tools by which existing governments could influence the choices available to them in governing an electronic world.

Policy Institutions affecting the Code

The main organization devoted to governing the Internet is the Internet Corporation for Assigned Names and Numbers (ICANN).[284] In its own words:

> . . . the growing international and commercial importance of the Internet has necessitated the creation of a technical management and policy development body that is more formalized in structure, more transparent, more accountable, and more fully reflective of the diversity of the world's Internet communities. In a phased, co-operative process, ICANN has been assuming responsibility to coordinate the stable operation of the Internet in four key areas: the Domain Name System (DNS); the allocation of IP address space; the management of the root server system; and the coordination of protocol number assignment.
>
> As a technical coordinating body, ICANN's mandate is not to "run the Internet." Rather, it is to oversee the management of only those specific technical managerial and policy development tasks that require central coordination: the assignment of the Internet's unique name and number identifiers.[285]

These "technical, managerial and policy development tasks" include how anyone can get access to the Internet, the rights to anonymity online, the cost of access, the types of permissible discussion, and other important elements of electronic communications. As a result, there has been a good deal of interest in who runs ICANN and how its decisions are made. A study committee constituted by ICANN has proposed a kind of representative democracy, extending perhaps even to political parties.[286] Outsiders have pushed in different directions, with a good deal of attention to the process of having ICANN broadly representative of the world of Internet users and accountable for social consequences of its decisions.[287] And, some critics have been candidates for the Board of Directors.[288] This is a discussion very much in progress.

The Canadian equivalent of ICANN is the Canadian Internet Registration Authority (CIRA),[289] which runs the *.ca* domain. CIRA governs registrars through which *.ca* domains are issued, and imposes a lengthy set of legal obligations on registrants.[290] CIRA, too, is in evolution, having just begun its function by taking over registration duties in November 2000. It held its first election for the Board of Directors in June 2001, and has created a dispute resolution policy on domain names.[291] Since CIRA runs one domain under the ICANN umbrella, it does not have as broad a policy or governmental impact as the latter body.

Another policy organization on a world scale is the World Intellectual Property Organization (WIPO).[292] WIPO is important to governance questions because it runs a domain-name dispute resolution system that is taking care of such disputes economically and generally to the satisfaction of the parties. It could be considered slightly like a court system for this aspect of the Internet; some domain name registration policies require the registrant to submit to the WIPO dispute resolution system before logging on.[293]

The biggest policy body involved in the Internet is still the United States government. Its historical role as governor of the defence computer system has not yet ended. Much of the regulation in later years has been done by the Department of Commerce, because of the interstate trade and the communications elements of the regulation. Some people say that ICANN itself can operate only if the U.S. government allows it to do so, and allege that the United States Constitution and federal statutes continue to govern the Internet. As a result, we see American congressional committees holding hearings about ICANN's processes,[294] and members of the Cabinet reviewing transactions about Internet administration.[295] Critics of ICANN who want it to be more representative and accountable through its election structure also seem comfortable, at least if they are Americans, in supporting political control through the U.S. government.[296]

Standards bodies

The thesis of this part of this paper is that standards themselves are not neutral, that the choices made by their designers have consequences in the political economy of the computer communications that the standards enable. These results may not be intended by their designers, who may not be aware of them. The work of the standards bodies goes on, necessarily. This is not the place to examine in detail their work. We will

provide here only a brief overview of some of the major players, to help situate the organizations that those interested in electronic government need to keep in mind.

Internationally, a list of the main bodies affecting the Internet may start with the Internet Society (ISOC), a non-profit organization that focuses on standards, public, policy, education and membership of the Internet.[297] ISOC sponsors the Internet Engineering Task Force (IETF),[298] which sets the basic inter-computer protocols that make the Internet work, and the Internet Research Task Force,[299] which does longer range research on technical topics of interest. The communications that these bodies are concerned with often occur over networks governed by rules set by the International Telecommunications Union,[300] which coordinates governmental and private sector telecom networks and services. Beyond this, there is the International Organization for Standardization (ISO),[301] which has recently spent considerable energy developing standards for electronic documents.

Many standards that influence authentication of electronic records, a crucial concern of electronic government,[302] are set in the United States by the National Institute of Science and Technology (NIST),[303] such as the "technology neutral" rules for electronic signatures, or the American National Standards Institute (ANSI),[304] whose Accredited Standards Committee X9 Financial Industry Standards Inc.[305] has defined the operation of digital signatures and certificates. Private standards are also influential, such as those of the Information Security Committee of the Science and Technology Section of the American Bar Association, whose Digital Signature Guidelines[306] set the tone for discussion of the subject for years, and whose new Public Key Infrastructure Appraisal Guidelines seem likely to do the same for PKI systems.[307] In Europe, the Information and Communications Technologies Standards Board[308] sponsors the creation of the European Electronic Signature Standard,[309] which people are looking to in order to make practical their compliance with the Electronic Signature Directive.[310]

In Canada, electronic documents and signatures have been the subject of discussions by the Standards Council of Canada,[311] the Canadian General Standards Board,[312] whose work on micrographics and electronic records as documentary evidence has been very influential,[313] and the Telecommunications Standards Advisory Council of Canada.[314] Many of these are encouraged by the Electronic Commerce Task Force run by Industry Canada.[315] Finally, the Quebec legislation on new technologies[316] provides a role for standards in general and the Bureau de normalisation du Québec[317] in particular in ensuring that electronic records to which Quebec law applies are reliable and consistent with best practices internationally.

It can be seen that the governing authorities for the development of standards for electronic communications are very diverse. Developing the thesis that their work constitutes a kind of law within which electronic government must operate, and which democratic government must be able to account for, will require a good deal of thought and practical politics in the future.

Conclusion

The terrain on which government is expected to do its job is not stable. Knowing who is doing what to whom, and how to make them stop doing it or do it some other way, presents a multitude of new challenges. However, it is clear that some of the traditional legal tools are still available, and the courts and administrative tribunals have found ways to assert authority over activities brought before them. It appears likely that less direct methods of controlling behaviour will prove fruitful to supplement the institutional regulators. The broader the level of behaviour, however, the less clear are the means of control — the electronic economy is harder to regulate at the macro level than individual businesses. Meanwhile the processes of government are evolving, along with its relationship with its citizens as citizens.

Questions of law merge with questions of political economy and questions of technology. For the moment, there seems limited potential for law reform in aid of the issues discussed in this paper. This does not exclude focused responses to particular problems, but governments will need prudence to ensure that their measures affect only the targets sought; the risk of spillover effects is high, and the legitimacy of the effort will be called into question. The ground needs to be clearer, and the potential of existing institutions and practices better explored, before broad new legislation is likely to be appropriate. Applying this thesis will be challenging, since the interests at stake are important. Governments are under pressure to do something. However, the CRTC has resisted that pressure so far for Internet regulation,[318] and more study seems the order of the day in issues in the electronic economy and electronic democracy.

Notes:

[1] Borders may be reappearing through newer technology, however. See *infra* at text accompanying note 106, and in general, B. Kahin and C. Nelson, eds., *Borders in Cyberspace* (Boston, MIT Press, 1999).

[2] See John D. Gregory, "Solving Legal Issues in Electronic Government: Authority and Authentication", (2002), 1 CJLT 1. For a useful list of issues with links to official sources, see Department of Justice (Canada), "Government On-Line: Checklist of Legal Issues" (2001), online: <http://canada.justice.gc.ca/en/ps/ec/gol.html>.

[3] See for example Castel, *Canadian Conflict of Laws* 4th ed. (Butterworths, Toronto, 1997) at 12.

[4] Within Canada, see for example the *Reciprocal Enforcement of Judgments Act*, R.S.O. 1990, c. R.5, a statute dating from the 1920s, and for a more recent approach, the *Uniform Enforcement of Canadian Judgments and Decrees Act*, [1997] Proceedings of the Uniform Law Conference of Canada 340, online: <http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1e4>.

[5] The current work of The Hague Conference on Private International Law on a multilateral convention on the recognition and enforcement of foreign judgments is described in detail at The Hague Conference's Web site, online: <http://www.hcch.net/e/workprog/jdgm.html>.

[6] J. Fontana, "E-mail's popularity creating a glut of legal issues", NetworkWorldFusion, October 30, 2000, online: <http://www.nwfusion.com/archive/2000/110227_10-30-2000.html>.

[7] For Canadian descriptions of the law, though mainly U.S. law, see Sookman, *Computer, Internet and Electronic Commerce Law*, (Toronto: Carswell, 2000) chapter 11, and Ogilvy Renault, "Jurisdiction and the Internet — Are Traditional Rules Enough?" (1998), online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4h>.

[8] *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D.Pa. 1997).

[9] (1998), 176 D.L.R. (4th) 46 (B.C.C.A.), online: <http://www.courts.gov.bc.ca/jdb-txt/ca/99/01/c99-0169.txt> and [1999] BCJ No. 622 (CA). Leave to appeal to the SCC denied, [2000] 1 S.C.R. vii.

[10] Michael Geist, "Is There a There There? Toward Greater Certainty for Internet Jurisdiction" (2001), online: <http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf>, which reviews the case law in detail.

[11] *Ibid.*

[12] Castel, *supra* note 3 at 593-4. The *Civil Code of Quebec* prevents the enforcement of an agreement by a consumer resident in Quebec to litigate disputes in any court but Quebec's: article 3149.

[13] *Rudder v. Microsoft*, [1999] 2 C.P.R. (4th) 474 (Ont. Sup. Ct.).

[14] *Supra* note 5.

[15] See for example Jamie Love, "What You Should Know about the Hague Conference on Private International Law's Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters", Consumer Project for Technology, June 2001, online: <http://www.cptech.org/ecom/jurisdiction/whatyoushouldknow.html>. The Hague Conference's Secretariat's summary in 2002, "The Impact of the Internet on the Judgements Project: Thoughts for the future", Prelim. Doc. No. 17, can be found at <ftp://ftp.hcch.net/doc/gen_pd17e.doc>.

[16] This is reflected in the Secretariat's "Reflection paper to assist in the preparation of a convention on jurisdiction and recognition and enforcement of foreign judgments in civil and commercial matters", Prelim Doc. 19, August 2002, accessible at <ftp://ftp.hcch.net/doc/jdgm_pd19e.doc>.

[17] U.S. Congressmen have, however, introduced the *Jurisdictional Certainty over Digital Commerce Act*, H.R. Bill 2421, First Session, 107th Congress, online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h2421ih.txt.pdf>. The bill gives the federal government exclusive authority, pre-empting state law, over transactions for goods and services sold and delivered online.

[18] *Morguard Investments v. de Savoye*, [1990] 3 S.C.R. 1077 says essentially that Canadian courts must recognize judgments from other Canadian courts where the originating court had a real and substantial connection with the case.

[19] *Uniform Court Jurisdiction and Proceedings Transfer Act*, Uniform Law Conference of Canada, 1994, online: <http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1c4>. It has been enacted in Saskatchewan (S.S. 1997, c. C-41.1) and the Yukon, S.Y. 2000, c. 7, but is not in force in either.

[20] The American Bar Association published a major study on the law and policy of Internet jurisdiction in 2000, online: <http://www.kentlaw.edu/cyberlaw/documents.html>. A report done for that study reviews Canadian law in particular: A. Gates, P. Tackaberry, A. Balinsky, "Canadian Law on Jurisdiction in Cyberspace", April 1999, online: <http://www.kentlaw.edu/cyberlaw/docs/rfc/canadaview.html>. For a perspective from the European Union, see the collection of documents online: <http://europa.eu.int/ISPO/ecommerce/legal/favorite.html>.

[21] C. Hart, "On-line Dispute Resolution and Avoidance in Electronic Commerce", Uniform Law Conference of Canada 1999, online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4e>.

[22] See the *Arbitration Act, 1991*, S.O. 1991 c. 17, and generally the *Uniform Arbitration Act*, [1990] Proceedings of the Uniform Law Conference of Canada 86, online: <http://www.ulcc.ca/en/us/arbitrat.pdf>. The *Statutory Powers Procedure Act*, R.S.O. 1990, c. s. 22 now provides for "electronic hearings" before administrative tribunals in Ontario. These provisions were added by S.O. 1994, c. 27, s. 56 and expanded by S.O. 1997, c. 23, s. 13.

[23] Ontario has a program of mandatory mediation in civil litigation. See the Rules of Civil Procedure, R.R.O. 1990, c. 194, Rule 24.1, made permanent by O. Reg. 244/01, *Ontario Gazette* July 7, 2001.

[24] Consumers International, "Disputes in Cyberspace: Online dispute resolution for consumers in cross-border disputes — an international survey" (December 2000), online: <http://www.consumersinternational.org/campaigns/electronic/disputes_in_cyberspace_2001.pdf>.

[25] Online: <http://www.consumersinternational.org/campaigns/electronic/sumadr-final.html>.

[26] The orientation document is online at: <http://www.oecd.org/pdf/M00001000/M00001595.pdf>. The papers presented can be found by searching "online trust workshop" in the Electronic Commerce section of the OECD Web site, <http://www.oecd.org>.

[27] See for example, online: <http://www.disputes.net/cyberweek2001/onlinebibliography.htm#articles>; <http://www.mediate.com/odr/>; and ODR News, <www.odrnews.com>. The United Nations Economic Commission for Europe held a forum on Online Dispute Resolution in June 2002, described online: <http://www.e-global.es/arbitration/papersadr/un_odr_june_2002.pdf>. The Australian Competition and Consumer Commission supported ODR in "Dispute Resolution in Electronic Commerce Discussion Paper", March 2002, online at: <http://www.accc.gov.au/ecom2/ecom_dispute_res.html>.

[28] Online: <http://www.law.washington.edu/ABA-eADR>.

[29] The draft report is online: <http://www.law.washington.edu/ABA-eADR/drafts/2002.04.05draft.html>. A summary of the responses to the draft report as of April 2002 is online: <http://www.law.washington.edu/ABA-eADR/documentation/docs/PrincipalViewsExpressed.pdf>.

[30] Online: <http://arbiter.wipo.int/domains>. The fairness of this process has been questioned. See M. Geist, "Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP" (2001), online: <http://aix1.uottawa.ca/~geist/geistudrp.pdf>, updated in March 2002 at <http://aix1.uottawa.ca/~geist/fairupdate.pdf> (March 2002).

[31] W.C. Graham, "The Internationalization of Commercial Arbitration in Canada: A Preliminary Reaction", (1987-88), 13 C.B.L.J. 2 at 2.

[32] See the Free Trade Agreement of the Americas, draft July 3, 2001, Chapter on Intellectual Property Rights: online: <http://www.ftaa-alca.org/ftaadraft/eng/draft_e.doc>.

[33] Online: <http://www.cira.ca/en/cat_Dpr.html>.

[34] See M. Geist, "The Reality of Bytes: Regulating Economic Activity in the Age of the Internet", 73 Washington Law Review 521 (1998), and C.T. Marsden, ed., *Regulating the Global Information Society* (London, Routledge, 2000).

[35] CRTC, New Media Decision, May 1999, online: <http://www.crtc.gc.ca/archive/eng/Notices/1999/PB99-84.htm>.

[36] *Ibid.* at para 46.

[37] *Ibid.* at paras 48–50.

[38] Online: <http://www.albertasecurities.com/DATA/items/EOL/orders/494580.pdf>. More recently the British Columbia Securities Commission sanctioned an online trader who was resident in B.C. *Re Jesse J. Hogan*, 2002 BCSECCOM 537, June 19, 2002, online at <http://

www.makeashorterlink.com/?Y2CA36F21>. The Commission refused to adopt a "different regulatory approach towards the internet" (para. 73).

[39] S.A. 1981, c. s.6.1, as amended.

[40] *Publication of Musical Works*, Decision on Tariff 22 — Transmission of a musical work to subscribers via a telecommunication service not covered under Tariff 16 or 17, Part 1: Legal Issues (1999), online: <http://www.cb-cda.gc.ca/decisions/m27101999-b.pdf>.

[41] *Ibid.* at table of contents.

[42] *Ibid.* at section III.

[43] *SOCAN v. Canadian Association of Internet Providers et al.*, [2002] FCA 166, May 1, 2002, online: <http://decisions.fct-cf.gc.ca/fct/2002/2002fca166.html>.

[44] *Ibid.* at para 163ff.

[45] *Official Records of the United Nations General Assembly, Fortieth Session, Supplement No. 17* (A/40/17), online at <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>.

[46] *Uniform Electronic Commerce Act* (UECA), [1999] Proceedings of the Uniform Law Conference of Canada 380, online: <http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1>.

[47] A list of implementing legislation in each jurisdiction is online at <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4b>.

[48] *Model Law* article 15; UECA section 23.

[49] *Model Law, Guide to Enactment*, *supra* note 45 at para 100.

[50] *Supra*, note 43 at para 186ff. See *infra*, text accompanying note 203, for the importance of the location of the server to taxability.

[51] The Church of Scientology alleged violation of its copyright on several instances apparently for this purpose. See T. Lyons, "Scientology or Censorship: You Decide", 1 *Rutgers Journal of Law and Religion* No. 2 (2001), online: <http://www-camlaw.rutgers.edu/publications/law-religion/scientology.htm>.

[52] *Twentieth Century Fox File Corp. v. iCraveTV, et al.*, 2000 U.S. Dist. LEXIS 1013 (W.D.Pe Jan 28, 2000). Similar litigation was pending in Canada, brought by Canadian broadcasters. See description below of the more recent JumpTV controversy, *infra* note 112.

[53] R. Naiberg, "Patent Protection for E-Commerce Inventions", (2000-2001), 2 I.E.C.L.C. 17.

[54] *Supra* note 15.

[55] Traditionally, the common law does not protect monopolies over information or expression, which are the essence of patents and copyright. The common law does protect trade names against unfair competition, though the *Trade-marks Act*, R.S.C. 1985, c. T-13, regularizes the protection. Trade secrets can be enforced through the courts, within limits.

[56] Governments' ability to do so is restricted by recent international conventions on data bases and other electronic elements of IP. The World Intellectual Property Organization (WIPO) developed two conventions in 1996, the Copyright Treaty, online: <http://www.wipo.int/clea/docs/en/wo/wo033en.htm>, and the Performances and Phonograms Treaty, online: <http://www.wipo.int/clea/docs/en/wo/wo034en.htm> (both accessed June 13, 2002). They are in force in several countries (see WIPO's lists online: <http://www.wipo.org/treaties/documents/english/word/s-wct.doc> for the Copyright Treaty and <http://www.wipo.org/treaties/documents/english/word/s-wppt.doc> for the Performances and Phonograms Treaty); Canada has signed them and is working on their implementation and ratification.

[57] Legislation was passed by the House of Commons in June 2002 to authorize regulations for retransmission rights by "new media retransmitters". *Act to amend the Copyright Act*, Bill C-48, online at: <http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-48/C-48_3/90174bE.html>. The CRTC called in July 2002 for public comment on Internet retransmissions of broadcast content. See <http://www.crtc.gc.ca/archive/ENG/Notices/2002/pb2002-38.htm>. Other legislation on copyright protection online is noted *infra* in text at note 120.

[58] *Citron et al., v. Zundel*, Canadian Human Rights Tribunal, January 18, 2002, online: <http://www.chrt-tcdp.gc.ca/decisions/docs/citron-e.htm>. The discussion of jurisdiction over the Internet is dealt with in paras 49–117.

[59] *Ibid.* at paras 64, 84, 108–110.

[60] *Mark Schnell and Canadian Human Rights Commission et al.*, August 20, 2002, online at <http://www.chrt-tcdp.gc.ca/decisions/docs/schnell-e.htm>. In this case, all the parties resided in British Columbia.

[61] For example, the *Consumer Protection Act*, R.S.O. 1990, c. C.31.

[62] For example, the *Travel Industry Act*, R.S.O. 1990, c. T.19.

[63] *Supra* text preceding note 34.

[64] See for example J.S. Ziegel, B. Geva and R.C.C. Cuming, *Commercial and Consumer Transactions: cases, text and materials*, (Toronto: Emond Montgomery, 1995), vol.1, Sales Transactions.

[65] For a general review of the problems of consumer protection in e-commerce, see the study by Roger Tassé and Kathleen Lemieux for Industry Canada, "Consumer Protection Rights in Canada in the context of electronic commerce", 1998, online: <http://strategis.ic.gc.ca/SSG/ca01028e.html>.

[66] *Principles of Consumer Protection for Electronic Commerce: A Canadian Framework*, Industry Canada, 1999, online: <http://strategis.ic.gc.ca/SSG/ca01180e.html>. The Principles call for protection for consumers shopping online equivalent to that available in traditional forms of commerce.

[67] Internet Sales Contract Harmonization Template (2001), online: <http://www.strategis.ic.gc.ca/ssg/ca01642e.html>. Provinces and territories have the responsibility for consumer protection in general, though the federal Office of Consumer Affairs at Industry Canada plays an active coordinating role.

[68] See for example Ontario's amendments to the *Consumer Protection Act*, in the *Red Tape Reduction Act*, 1999, S.O. 1999, c. 12, Sched. F, ss. 15, 45(2), and O. Reg. 175/01. The provisions conform with a harmonization template adopted by a federal–provincial–territorial working group in 1995.

[69] *Ibid.* at ss. 3 and 4.

[70] The consumer must act relatively quickly to exercise the rescission right. *Ibid.*, s. 5.

[71] *Ibid.* at s. 11.

[72] *Electronic Commerce and Information Act*, S.M. 2000, c. E55, amending the *Consumer Protection Act*, C.C.S.M. c. C200. These provisions, and regulations in support, came into force on March 19, 2001.

[73] Alberta's Internet Sales Contract Regulation, made under the *Fair Trading Act*, S.A. 1998, c. F-1.05., A.R. 81/2001, made in May 2001. It is online: <http://www.qp.gov.ab.ca/Documents/REGS/2001_081.CFM>.

[74] Alberta's statute, *supra* note 73, says that its rules apply when the consumer or the supplier are in Alberta.

[75] See "The Determination of Jurisdiction in Cross-border Business to Consumer Transactions: A Discussion Paper", published by Industry Canada in the summer of 2002 as a product of the working group that produced the earlier template, with input from the Uniform Law Conference, online at <http://strategis.ic.gc.ca/pics/ca/consultation-02mainapp-eng.pdf>.

[76] *Charter of the French Language* (Bill 101), S.Q. 1977, c. 5, as amended, Title I, Chapter VII, notably ss. 52 and 58.

[77] Office of the French Language (Quebec), "The Charter of the French Language and Web Sites", online: <http://www.olf.gouv.qc.ca/english/faqs/faqs_anglais.html#frequently>.

[78] *Procureur Général du Québec c. Hyperinfo Canada Inc.*, November 1, 2001, file 550-61-000887-014, online at: <http://www.jugements.qc.ca/cq/200111fr.html>; *Procureur Général du Québec c. Waldie-Reid*, May 23, 2002, file 760-61-026203-019, online: <http://www.jugements.qc.ca/c2/200205fr.html>. In both cases, the defendants were located in Quebec and the Web sites initially targeted the Quebec market, though the Hyperinfo site attempted to block addresses with "qc" from accessing the site and noted on the site that the site was not to be used by Quebec residents.

[79] Public Law No. 106-229, 114 Stat. 464 (2000) (codified as 15 U.S.C. §§ 7001-7006, 7021, 7031) (enacted S. 761); available online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf>.

[80] A request for similar legislation in Canada was addressed to provincial Ministers of Justice and Attorneys General by the Public Interest Advocacy Centre (PIAC) in connection with the adoption of the *Uniform Electronic Commerce Act*. PIAC letter, June 2000, online: <http://www.piac.ca/uecalet.htm>. To date, the request has had no discernable impact.

[81] The Federal Trade Commission held a workshop on the consumer protection provisions of E-SIGN in April 2001. Public submissions and transcripts are online: <http://www.ftc.gov/bcp/workshops/esign/index.html>.

[82] See Federal Reserve Board press release and attachments, online: <http://www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329/>.

[83] *Ibid.*

[84] Adopted by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in 1999 and available online: <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>. See John D. Gregory, "The UETA and the UECA: Canadian Reflections", (2001) 37 Idaho L.R. 441.

[85] More discussion of state laws appears at <http://www.uetaonline.com>.

[86] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers with respect to distance contracts, online: <http://europa.eu.int/ISPO/ecommerce/legal/documents/31997L0007/31997L0007_en.html>. See also proposal for its revision, *infra* note 89, notably part 4, articles 5ff.

[87] See Amended proposal for a European Parliament and Council Directive concerning the distance marketing of consumer financial services . . . , COM (1999) 385 final, Brussels, 1999, online: <http://europa.eu.int/eur-lex/en/com/pdf/1999/en_599PC0385.pdf>, which noted (at page 10) that the controversial amendment to Article12 was withdrawn as contrary to the Brussels Convention on the Recognition and Enforcement of Judgments in Civil and Commercial Matters. See also Ann Salaun, "Consumer Protection Issues" in the Electronic Commerce Legal Issues Platform (2001), <http://europa.eu.int/ISPO/legal/en/lab/991216/consumer_protection.doc>.

[88] Paul Mellor, "Europe Proposes Dual Plan on Disputes in Commerce", New York Times, May 4, 2002, online: <http://www.nytimes.com/2002/05/04/business/worldbusiness/04EURO.html>.

[89] 2000/31/EC. Online: <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf>.

[90] *Ibid.* at article 19.

[91] *Ibid.* at article 3.

[92] Roger Tassé and Maxime Faille, "Online Consumer Protection: A Study of Regulatory Jurisdiction in Canada", Office of Consumer Affairs, Industry Canada, Ottawa, 2001. Online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4n>.

[93] *Ibid.*, "Recommendations".

[94] Canadian privacy legislation, both the federal statute, the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Part 1, and the Quebec legislation, *An Act respecting the protection of personal information in the private* sector, S.Q. 1993, c. 17, apply to online and offline communications without distinction. "Online privacy" rules do not meet all the needs of a society based on electronic communications.

[95] OECD 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data have been the basis for almost all world-wide rules on privacy protection for public or private sectors, online: <http://www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.html>.

[96] Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data. Online: search at <http://europa.eu.int/eur-lex/en/search/search_lif.html> for Directive, year 1995, document 46.

[97] *Ibid.* at articles 25 and 26.

[98] For one explanation among many, see MerchantInfoWeb.com; ''Merchant Accounts'' (undated), online: <http://www.merchantinfoweb.com/merchant-accounts.htm>.

[99] See discussion of the Manitoba legislation *supra* note 72. Consumer groups have supported mandatory chargeback. See Public Interest Advocacy Centre, "Comparative Review of Laws and Voluntary Codes relating to certain aspects of Consumer Protection in Electronic Commerce", study commissioned by Industry Canada, November 1999, pp. 10–27, online: <http://www.piac.ca/newpage21.htm>.

[100] To date, the card issuers that are banks have not argued that they can be regulated only by the federal government, not the provinces that are implementing the template's rules, though the chargeback rules affect their relations with their customers.

[101] In the United Kingdom, a service provider was found liable for defamation once put on notice of the nature of the material being transmitted. *Godfrey v. Demon Internet Limited*, [1999] 4 All E.R. 342, [2001] Q.B. 201. Online: <http://www.cyber-rights.org/documents/godfrey_decision.htm>. The *Defamation Act 1996* (U.K.), section 1, sets out the conditions for a defence of innocent dissemination. It is arguable that the common law on the point, as in effect in Canada, would permit a different result.

[102] J. Borland., "File-trading pressure mounts on ISPs", C/Net News.com, July 25, 2001, online: <http://news.com.com/2100-1033-270568.html>. See also *supra* note 51.

[103] *An Act to establish a legal framework for information technology*, S.Q. 2001, c. 32, online: <http://publicationsduquebec.gouv.qc.ca/fr/cgi/telecharge.cgi/161A0129.PDF?table=gazette_pdf&doc=161A0129.PDF&gazette=4&fichier=161A0129.PDF>. Sections 36 and 37 exempt ISPs if they act as intermediary, subject to certain qualifications.

[104] *Supra* note 40.

[105] The *Communications Decency Act*, 47 U.S.C. s. 230. The provision was given effect notably in *Zeran v. AOL* , 129 F.3d 327 (U.S.C.A. 4th, 1997), cert. denied, 524 US 937 (1998), online: <http://laws.lp.findlaw.com/4th/971523p.html>. Criminal liability is dealt with *infra* in text accompanying note 145.

[106] See the Guardian, July 11, 2001, "Internet Firm Wins Bulger Protection", online: <http://www.guardian.co.uk/internetnews/story/0,7369,519930,00.html> and a comment, "Nobody Rules OK", the Guardian, July 16, 2001, online: <http://www.guardian.co.uk/internetnews/story/0,7369,522238,00.html>.

[107] *Supra* note 89 at article 12.

[108] Telecom Decision 99-11, online: <http://www.crtc.gc.ca/archive/eng/Decisions/1999/DT99-11.htm>.

[109] *AT&T Corp. v. City of Portland*, 216 F. 3d. 871 (U.S.C.A 9th 2000), finding that a municipality could not require the cable company to provide access to competing service providers.

[110] See *MediaOne Group, Inc. et al. v. County of Henrico,Virginia*, 251 F.3d 356 (U.S.C.A. 4th 2001), online: <http://laws.lp.findlaw.com/getcase/4th/case/001680Pv2&exact=1>. The court held that a county could not require the cable company to give access to competing ISPs because this was a matter of pre-emptive federal statute.

[111] Federal Communications Commission, Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 65 Fed. Reg. 60,441 (2000).

[112] JumpTV, online: <http://www.jumptv.com>, is counting on doing this. Its full scale operation has been delayed by a change of business model, however. JumpTV hopes to avoid the fate of iCraveTV, which a U.S. court did not believe could restrict its accessibility enough to avoid violating U.S. copyright law. *Supra* note 52. Similar litigation was pending in Canada, brought by Canadan broadcasters. The legislative terrain has also been evolving in this field. *Supra* note 57.

[113] Stefanie Olsen, "Yahoo ads close in on visitors' locale", CNET News.com, June 27, 2001, online: <http://news.com.com/2102-1023-269155.html>.

[114] The alleged ability to do this, based on expert advice, influenced the French court that ordered Yahoo.fr to block auctions of Nazi memorabilia from French Internet users, as such auctions broke French law. See K.McCarthy, "Yahoo! Nazi tech expert backtracks", The Register, November 28, 2000, online: <http://www.theregister.co.uk/content/6/15063.html>. The case is noted further *infra* note 159.

[115] See Michael Geist, "E-borders loom, for better or worse", *The Globe and Mail*, June 28, 2001, online: <http://news.globetechnology.com/servlet/GAMArticleHTMLTemplate?tf=globetechnology/TGAM/NewsFullStory.html&cf=globetechnology/tech-config-neutral&slug=TWGEISY&date=20010628>.

[116] The Federal Communications Commission in the United States held hearings on this subject in 2000, in response to a petition by wireless device manufacturers for rulemaking on "fair location practices". See the notice of hearing, March 2001, online: <http://www.fcc.gov/Bureaus/Wireless/Public_Notices/2001/da010696.html>.

[117] J. Borland, "Copy-protected CDs quietly slip into stores", C/Net News.com, July 18, 2001, online: <http://news.cnet.com/news/0-1005-200-6604222.html>.

[118] Sandeep Junnarkar, "Horrors for publishing industry: King's e-book cracked", C/Net News.Com, March 31, 2000, online: <http://news.cnet.com/news/0-1005-200-1618243.html>.

[119] The anti-copying programs were published under the heading Secure Digital Music Initiative (SDMI), online: <http://www.sdmi.org>.

[120] *Digital Millennium Copyright Act*, Public Law 105-304, 1998, online summary: <http://www.loc.gov/copyright/legislation/dmca.pdf>. The

first arrest for preparing software to break codes on electronic books was reported in July 2001. A U.S. government press release of December 2001 about the ensuing prosecution appears online: <http://www.cybercrime.gov/sklyarovAgree.htm>. A scientist who claims to have broken the SDMI security routines now says he is prevented from publishing this research because of the anti-avoidance provisions of the DMCA, and has started a lawsuit against the Recording Industry Association of America to get the right to publish. The legal documents are online: <http://www.eff.org/Legal/Cases/Felten_v_RIAA/felten_legal_documents.html>.

[121] *Record Industy of America v. Napster*, July 11, 2001. "Court: Napster Filters Must be Foolproof", CNET News.Com, online: <http://news.cnet.com/news/0-1005-200-6549898.html>, reversed on appeal, "Napster Gets Last-Minute Reprieve", C/Net News.Com, July 18, 2001, online: <http://news.cnet.com/news/0-1005-200-6605948.html>.

[122] American Uniform Statutes are online. For all versions of UCITA, see online: <http://www.law.upenn.edu/bll/ulc/ulc.htm#ucita>. The self-help provision was section 816 (called "Limitations on Self-Help").

[123] For criticisms of UCITA and relevant texts, see UCITAONLINE, online: <http://www.ucitaonline.com>.

[124] The 2000 amendments to s. 816 prohibited self-help in "mass market transactions". <http://www.law.upenn.edu/bll/ulc/ucita/ucitaAMD.htm>.

[125] *Théberge v. Galérie d'Art du Petit Champlain Inc.*, 2002 SCC 34, online: <http://www.lexum.umontreal.ca/csc-scc/en/rec/html/laroche.en.html>, para. 31.

[126] "Digital Rights: Background, Systems, Assessment", February 14, 2002, online: <http://europa.eu.int/information_society/newsroom/documents/drm_workingdoc.pdf>.

[127] *Supra* note 66.

[128] *Ibid.*

[129] Online: <http://www.safeshopping.org>.

[130] See for example the Securities Exchange Commission (U.S.), "The Internet and Online Trading" (2001), online: <http://www.sec.gov/investor/online.shtml>.

[131] Online: <http://www.osc.gov.on.ca/en/games/spot_the_bull/index.htm>.

[132] Federal Trade Commission, "Consumer Protection: E-Commerce & the Internet", online: <http://www.ftc.gov/bcp/menu-internet.htm>.

[133] While this article does not purport to be a thorough canvass of the literature, it seems appropriate here to note some of the early thinking on this aspect of the jurisdiction/regulation problem, by David Post and David Johnston in the United States, e.g., "Law & Borders", (1996) 48 *Stanford L.R.* 1367, and Henry Perritt, "Cyberspace and State Sovereignty", (1997) 3 J.Int'l Leg.Studies 155; and in Canada by Pierre Trudel, *Le droit du cyberespace* (Montreal, Thémis, 1998) and by Messrs Racicot, Hayes, Szibbo and Trudel. "The Cyberspace is not a 'No Law Land': A study of the issues of liability for content circulating on the Internet", Industry Canada 1997, online: <http://strategis.ic.gc.ca/pics/sf/1503118e.pdf>.

[134] Michael Geist, "Consumer Protection and Licensing Regimes Review: the Implications of Electronic Commerce" (2000), online: <http://aix1.uottawa.ca/~geist/mccrgeist.pdf>.

[135] David Post, "Betting on Cyberspace", The American Lawyer (June 1997), online: <http://www.temple.edu/lawschool/dpost/Gambling.html>.

[136] America Online, "Total Satisfaction", online: <http://www.aol.com/amc/total_satisfaction.html>.

[137] Online: <http://pages.ebay.com/help/community/insurance.html>.

[138] Online: <http://www.squaretrade.com/spl/jsp/eby/eb.jsp?marketplace_name =ebay&campaign=EBY_OD_6>.

[139] Online: <http://www.bbbonline.com>.

[140] Online: <http://www.webtrust.org>.

[141] Online: <http://www.truste.com>.

[142] John D. Gregory, "Self-Regulation or Government Intervention: Issues and Frameworks for Law Reform in Electronic Commerce", in *The Electronic Evolution: Business and Law Adapt to New Realities*, (Queen's Annual Business Law Symposium [1998], Kingston, 2000) 108. Online: <http://www.euclid.ca/queens.html>.

[143] See *infra*, text following note 270 and especially accompanying note 297.

[144] This is not the place to discuss the distinction between criminal activity, a matter of federal legislation in Canada, and activity prohibited by law, which may be provincially proscribed as well. The margins may be debated, but the core activities are not ambiguous.

[145] See sections 342.1 and 342.2 of the *Criminal Code of Canada*, R.S.C. 1985, c. C-46 as amended by S.C. 1985, c. 27 (first supp), s. 45, and by S.C. 1997, c. 18, ss. 18, 19.

[146] The classic case is that of the Philippine author of the ILOVEYOU virus. Despite creating worldwide damage to many computers, he was not guilty of anything under Philippine law at the time. See "Philippines Sets New Cyber Law", ABC News.com, June 15, 2000, online: <http://abcnews.com/sections/tech/DailyNews/virus000615.html>. The Commission of the European Union has issued a report to the European Parliament calling for updated criminal laws: "Creating a safer information society by improving the security of computer information infrastructure and combating computer-related crime", Document COM (2000) 890, January 26, 2001; response by Parliament of September 2001 in Official Journal 21.03.2002, p. C72E/321.

[147] McConnell International, "Security Law Project" (2000), online: <http://www.mcconnellinternational.com/services/securitylawproject.cfm>.

[148] *Cybercrime Act 2001*, online: <http://www.austlii.edu.au/cgi-bin/disp.pl/au/legis/cth/consol%5fact/ca2001112/?query=title+%28+%22cybercrime+act+2001%22+%29>.

[149] United States Department of Justice, Computer Crime and Intellectual Property Section, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (2001), online: <http://www.cybercrime.gov/searchmanual.htm>.

[150] See the *Criminal Law Amendment Act 2001*, Bill C-15, 2001. Section 94 of the Bill adds Part XXVIII to the *Criminal Code*, dealing with electronic documents, obtaining search warrants and informations by electronic communication between police and justices of the peace, and the like. Online: <http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-15/C-15_1/90148bE.html>.

[151] A comprehensive view of criminal law issues in e-commerce appears on the United States Department of Justice Web site, <http://www.cybercrime.gov>.

[152] *Criminal Code of Canada*, *supra* note 145, s. 7. The limits to the child sex offence prosecutions authorized in ss. 7(4.1) are described in "Child Sex Tourism Fact Sheet", published in 1999 by the Department of Foreign Affairs and International Trade (Canada), online: <http://www.voyage.gc.ca/Consular-e/Publications/child_fact-e.htm>.

[153] *Minnesota (State of) v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (Minn.C.A.1997).

[154] The state had its own lottery, with its own Web site. Online: <http://www.lottery.state.mn.us/index.html>. One wonders if the desire to reduce competition played any part in the decision to prosecute.

[155] *Supra* note 145 at s. 207.

[156] *Re Earth Future Lottery (P.E.I.)*, 2002 PEISCAD 8, online: <http://www.gov.pe.ca/courts/supreme/reasons/923.pdf>.

[157] In any event, the Code prohibited lotteries operated through a computer, and using the Internet qualified, even though the Earth Fund planned to make the draws themselves by hand in P.E.I. For a critical note on the case, see M. Geist, "Web lottery case misses the jackpot", *Globe and Mail*, Toronto, May 2, 2002, online at <http://www.theglobeandmail.com/servlet/ArticleNews/printarticle/gam/20020502 /TWGEIS>.

[158] *Ibid.* at para. 14.

[159] *L'Union des Etudiants juifs en France et la Ligue contre le racisme et l'antisémitisme c. Société Yahoo! Inc et Société Yahoo! France*, Tribunal de Grande Instance de Paris, May 22, 2000, online: <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=129>.

[160] *Supra* note 114.

[161] For an anti-censorship view, see R. Corn-Revere, "Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?", Cato Institute, Washington , D.C., July 2002, online: <http://www.cato.org/pubs/briefs/bp71.pdf>.

[162] The French court made its compliance order only against Yahoo! Inc, not against Yahoo! France, which complied with French law for its own content. A California court has refused in advance to enforce a French order against Yahoo in this matter. *Yahoo! Inc. v. La Ligue contre le*

Racisme et l'Antisemitisme, 169 F. Supp. 2d1181 (N. D. Cal. 2001). The decision has been appealed.

[163] *Supra* note 99 and accompanying text.

[164] *Internet Gambling Payments Prohibition Act*, H.R. 2579, introduced in July, 2001. A previous attempt at such legislation failed. *Internet Gambling Funding Prohibition Act*, H.R.4419, 2000, online: <http://techlawjournal.com/cong106/gambling/hr4419ih.htm>. There is some evidence that the strategy is working: J. Doward, "Dotcom's casino disaster", Guardian Unlimited, April 7, 2002, online: <http://www.guardian.co.uk/internetnews/story/0,7369,680072,00.html>.

[165] Unless one is selling goods prohibited on moral or social grounds, as in the Yahoo! case.

[166] Federal Trade Commission, "Fighting Consumer Fraud: New Tools of the Trade" (1998), online: <http://www.ftc.gov/reports/fraud97/index.html>.

[167] Ontario Securities Commission, "OSC Takes Part in International Initiative against Internet-Based Securities Fraud", June 28, 2001. Online: <http://www.osc.gov.on.ca/en/About/News/NewsReleases/2001/nr_20010628_osc-initagainstfraud.htm>.

[168] Australian Competition and Consumer Commission, "The global enforcement challenge — The enforcement of consumer protection laws in a global marketplace — Discussion Paper" (1997), online: <http://www.accc.gov.au/docs/global/httoc.htm>, notably chapter 7.

[169] Council of Europe, Convention on Cybercrime, November 2001, online: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. Explanatory material is online: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[170] See for example the Global Internet Liberty Campaign, "Letter on Council of Europe Cybercrime Convention" (October 2000), online: <http://www.gilc.org/privacy/coe-letter-1000.html>, and its sequel written in December 2000, online: <http://www.gilc.org/privacy/coe-letter-1200.html>.

[171] Department of Justice (Canada), "Legal Access — Consultation Document", August 25, 2002, online at <http://canada.justice.gc.ca/en/cons/la_al/index.html>.

[172] See the Worldwide E-Commerce Fraud Prevention Internetwork, online: <http://www.merchantfraudsquad.com>.

[173] *Criminal Code of Canada*, *supra* note 145, ss. 318–320.

[174] Draft First Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, PC-RX(2002)15E, April 2002, online: <http://www.coe.int/T/E/Legal%5FAffairs/Legal%5Fco%2Doperation/Combating%5Feconomic%5Fcrime/Cybercrime/Racism_on_internet/PC-RX(2002)15E-11.pdf>.

[175] Computers still cannot appraise context very well, however, so stories abound of information being blocked for using a word that in context was perfectly appropriate. The effectiveness of filters is beyond the scope of this article. A recent study by an agency of the National Research Council in the U.S. found technology to be limited in its ability to protect youth from pornography. Computer Science and Technology Board, *Youth, Pornography and the Internet*, (2002), online: <http://books.nap.edu/books/0309082749/html/index.html>.

[176] *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*, 24 F. Supp. 2d 552 (E.D.Va. 1998), online: <http://www.eff.org/Legal/Cases/Loudoun_library/HTML/19981123_opinion_order.html>.

[177] *Ibid.*

[178] *Children's Internet Protection Act*, 47 U.S.C. 254(h) and 20 U.S.C. s. 9134.

[179] *The American Library Association et al. v. United States*, United States Court for the Eastern District of Pennsylvania. Pleadings are online: <http://www.ala.org/cipa/cipacomplaint.pdf> and the decision in favour of the plaintiffs at: <http://news.findlaw.com/cnn/docs/ala/cipa53102ord.pdf>.

[180] CRTC decided not to regulate spam as part of its general new media decision, *supra* note 35. For a note on its application to spam, see the National Post's report at the Electronic Frontier Foundation of Canada's site, online: <http://insight.mcmaster.ca/org/efc/pages/media/nationalpost.18may99a.html>.

[181] Trust.e, the Web site certification service noted at *supra* note 141, is participating in a spam protection system as well. Announcement of August 2002, online: <http://www.truste.org/about/MailShell_FINAL.html>.

[182] The right of an ISP to cancel the contract of a customer that violated the IPS's no-spam rule was upheld in *126763 Ontario Inc v. Nexx Online Inc.*, [1999] O.J. No. 2246 (Sup. Ct.), (1999), 45 O.R. (3d) 40. The decision referred both to the contract and to "Netiquette", the community values of Internet users. A U.S. court has reached a similar decision: *MonsterHut Inc. v. PaeTec Communications, Inc.*, N.Y. Supreme Court, App. Div., May 3, 2002, online: <http://www.courts.state.ny.us/ad4/Court/Decisions/2002/05-03-02/RTF/0613.rtf>. A French decision to the same effect was given in early 2002: *Monsieur P.V. c. Libertry Surf et Société Free*, Tribunal de grande instance de Paris, 15 janvier 2002, online at: <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=260>. The virtual communities referred to in *supra* note 133 may develop law enforceable in real courts.

[183] See the collection of cases on unsolicited e-mail at the John Marshall Law School Web site, online: <http://www.jmls.edu/cyber/cases/spam.html>. Some non-statutory lawsuits by computer users and network operators against spammers seem to have produced damage awards in the United States. See the AP story, "Fed up with unsolicited e-mail, computer users go to court", January 13, 2002, online: <http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2002/01/12/state1549EST0067.DTL&type=tech>.

[184] *State of Washington v. Jason Heckel doing business as Natural Instincts*, 24 P.3d 404 (Wash. S.C. 2001), cert. denied Oct. 29, 2001. Online by searching "Jason Heckel" at <http://www.legalwa.org>.

[185] For example, see the *Unsolicited Commercial Electronic Mail Act* of 2001, H.R 718. Online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h718rh.txt.pdf>.

[186] The Directive on privacy and electronic communications, 2002/58/EC, was adopted in July 2002. Article 13 requires prior consent of the recipient of electronic mail, subject to some qualifications. The parts on spam are excerpted at <http://www.euro.cauce.org/en/amendments1a.html#ftext>. For the anti-spam view of the debate, see the European wing of the Coalition Against Unsolicited Commercial E-Mail (CAUCE), online: <http://www.euro.cauce.org/en/news.html>.

[187] The arguments are reported in the press. See T. Richardson, "Europe Holds Key Vote on Spam Tomorrow", The Register, July 10, 2001, online: <http://www.theregister.co.uk/content/23/20290.html>.

[188] Notably the reference to European Union directives, *supra* note 89. For more on the EU e-commerce directive and harmonization of related European law, see Proceedings of the Workshop on Implementation of the E-Commerce Directive: Contract Law, Electronic Commerce Legal Issues Platform, December 2001, online: <http://www.eclip.org/workshop/10th/contract_law.htm>.

[189] *Infra*, text accompanying notes 297.

[190] See S. Chinoy, "Electronic Money in Electronic Purses and Wallets", (1997), 12 B.F.L.R. 15.

[191] See <http://www.mondex.ca> for general information. Trials in Sherbrooke, Quebec and in Guelph, Ontario have been wound up.

[192] *Ibid.*

[193] For details see online: <http://www.moneo.net>.

[194] B. Crawford, "Is Electronic Money Money?", (1997), 12 B.F.L.R. 399, online: <http://www.mccarthy.ca> under Publications, Crawford. Footnote 14 of that paper lists some significant sources of thinking on the subject at the time of writing.

[195] See for example the Bank of Nova Scotia's electronic payment system, online: <http://www.e-scotia.com>, and Canada Post's e-post system for payments, online: <http://www.epost.ca>.

[196] A. Creed, "E-Money to be made Legal Tender in Singapore", December 26, 2000, online: <http://www.infowar.com/p_and_s/00/p_n_s_122600c_j.shtml>.

[197] Ministry of National Revenue (now Canadian Customs and Revenue Agency), *Electronic Commerce and Canada's Tax Administration*, (Ottawa, MNR, 1998), online: <http://www.ccra-adrc.gc.ca/ecomm>. More recently, CCRA published *GST/HST and electronic commerce*, (2002), online: <http://www.ccra-adrc.gc.ca/tax/technical/ecommerce-e.html>.

[198] A list appears online: <http://www.oecd.org/EN/about/0,,EN-about-101-3-no-no-no-101,00.html>. See also Richard Doernberg, Walter Hallerstein, Luc Hinnekens and Jinyan Li, *Electronic Commerce and Multijurisdictional Taxation*, (Kluwer Law International, Amsterdam, 2001).

[199] See for example the *Retail Sales Tax Act*, R.S.O. 1990, c. R.31.

[200] *Excise Tax Act*, R.S.C. 1985, c. E-15.

[201] Robert Hettinga, an attorney in Boston, has said that the advent of strong financial cryptography means the end of the nation state as we know it. See "Re Digital Bearer Documents — an Oxymoron?" on the cryptography list archives, February 15, 1999, online: <http://www.privacy.nb.ca/cryptography/archives/cryptography/html/1999-02/0110.html>. He thought that this was good news. Most governments, and those they support and protect, will disagree.

[202] *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.), s. 245.

[203] See for example Jinyan Li, "Rethinking Canada's Source Rules in the Age of Electronic Commerce", (1999), 47 Can.Tax J. 1077–1125, 1411–1478.

[204] OECD, Clarification on the Application of the Permanent Establishment Definition in E-Commerce: Changes to the Commentary on the Model Tax Convention on Article 5, December 2000, online: <http://www.oecd.org/pdf/M000015000/M00015535.pdf>.

[205] Some doubt remained, depending partly on the degree of development of the activity at the server (*ibid.* at para 14) and partly on the policy view of the participant in the working group (*ibid.* at para 15).

[206] *Ibid* at para 7.

[207] Internal Revenue Department, Hong Kong, *Departmental Interpretation & Practice Notes, No. 39, Profits Tax, Treatment of Electronic Commerce*, July 2001, online: <http://www.info.gov.hk/ird/eng/pdf/ipn39.pdf>.

[208] OECD, "Tax Treaty Characterization Issues Arising from E-Commerce", February 1, 2001. Online: <http://www.oecd.org/pdf/M000015000/M00015536.pdf>.

[209] I am indebted to Professor Jinyan Li of Osgoode Hall Law School for the discussion of characterization issues. Correspondence with the author dated July 19, 2001.

[210] See for example the *Internet Tax Freedom Act*, 47 U.S.C. § 151 s. 1102. The previous statute expired in October 2001; a number of replacement statutes were introduced. Some bills banned only access taxes, some extended to sales and use taxes. K. Perine, "Bill Would Ban Net Access Taxes'', The Standard, July 17, 2001, online: <http://www.thestandard.com/article/0,1902,27992,00.html>. The ban was eventually extended by the *Internet Tax Non-Discrimination Act*, H.R.1552, signed November 28, 2001.

[211] A special working group of state representatives and business people in the United States could not arrive at a consensus in April 2001, but a majority favoured ending the moratorium on taxes on e-commerce. Online: <http://www.ecommercecommission.org>.

[212] See D. McCullough, "Vexing Questions about Net Tax", *Wired News*, May 12, 2001, online: <http://www.wired.com/news/politics/0,1283,43740,00.html>.

[213] See the background document for the European Union's Economic and Financial Committee (Ecofin) meeting of June 2001, online: <http://www.eu2001.se/eu2001/news/news_read.asp?iInformationID=15516>.

[214] Program delivery raises different questions, as noted briefly *supra*, text accompanying note 2.

[215] See a list of the Web sites online: <http://www.e-laws.gov.on.ca/relatedSites_E.asp?lang=en>.

[216] Online: <http://www.canlii.org>, modelled on the Australasian Legal Information Institute, online <http://www.austlii.edu.au>.

[217] Online: <http://www.e-laws.gov.on.ca/disclaimer_E.asp?lang=en>.

[218] The *Evidence Act*, R.S.O. 1990, c. E.23, s. 25.

[219] S.C. 2000, c. 5.

[220] R.S.C. 1985, c. C-5.

[221] R.S.C. 1985, c. S-22.

[222] *Supra* note 221 at subsection 10(2).

[223] *Supra* note 221 at subsection 6(3).

[224] R.S.C. 1985, c. S-20.

[225] *Supra* note 219, at ss. 61–70.

[226] *Ibid.* at s. 12.

[227] R.S.C. 1985, c. S-21, s. 3.

[228] *Legislation Revision and Consolidation Act*, *supra* note 225, subsections 31(2) and (3). This could be called "outsourcing the signature". An official binding text remains on paper, in known custody and recoverable if needed.

[229] See online: <http://laws.justice.gc.ca/en/note.html>.

[230] See for example <http://www.ontariocourts.on.ca>, which offers only Court of Appeal decisions so far; <http://www.courts.gov.bc.ca>, and the Supreme Court of Canada site at <http://www.scc-csc.gc.ca>.

[231] Canadian Association of Law Librarians, *"The Official Version": A National Summit to Solve the Problems of Authenticating, Preserving and Citing Legal Information in Digital Form*, online: <http://www.callacbd.ca/1997summit/index.html> (accessed July 20, 2001).

[232] The Canadian Citation Committee, *A Neutral Citation Standard for Case Law*, (1996, amended to December 2000), online: <http://www.lexum.umontreal.ca/citation/en/standard/standard.html>.

[233] See for example the *Archives Act*, R.S.O. 1990, c. A.27.

[234] Ian E. Wilson, "The End of History?", address to the conference "Electronic Democracy Ontario: Access to Records", Toronto, 1996. The author was then the Archivist of Ontario and is now the National Archivist of Canada. See also National Archives of Canada, *The Keeping of Business Records for Law, Audit and Archives: A Report on the Experts' Meeting*, (Ottawa, National Archives of Canada, 1999).

[235] Archives Canada, *Guidelines for Records Created Under a Public Key Infrastructure Using Encryption And Digital Signatures*, September 2001, online: <http://www.archives.ca/06/0618_e.html>.

[236] "Records Management Guidelines for Agencies Implementing Electronic Signature Technologies'' (October 2000), <http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html>.

[237] *Ibid.*, section 4.

[238] Notorious problems of machines of various vintages were widely reported after the 2000 American presidential election. The City of Toronto in November 2000 used machines that tallied the votes electronically and remitted them online to the counting computer after polls closed, allowing results in minutes, without problems. The decision to buy the machines is online: <http://www.city.toronto.on.ca/legdocs/1999/minutes/council/cc990928.htm>, item 10.67.

[239] For a report from the company that sold the machines, see online: <http://www.election.com/uk/political/arizona>.

[240] H. Geser, "Electronic Voting Projects in Switzerland", Sociology in Switzerland Online Publications, August 2002, online: <http://socio.ch/intcom/t_hgeser12.htm>.

[241] S.O. 2000, c. 17.

[242] *Ibid.*, s. 30.

[243] R.S.O. 1990, c. E.7.

[244] See for example *The Bell*, an online publication subtitled "Privacy, Security and Technology in Internet Voting", online: <http://www.thebell.net> and <http://www.elections.org>. Voting machine manufacturers are participating through the Internet Voting Technology Alliance, online: <http://www.ivta.org>. The Brookings Institute in the U.S. held a symposium in January 2000 on the Future of Internet Voting, online: <http://www.brook.edu/dybdocroot/comm/events/20000120.htm>. A recent study in the United Kingdom recommends further study of security aspects before implementing e-voting. Electoral Reform Society, *Elections in the 21st century: from paper ballot to e-voting*, (2002), introduction and summary online: <http://www.electoral-reform.org.uk/publications/books/exec.pdf>.

[245] See for example <http://www.liberal.ca>; <http://www.canadianalliance.ca>; <http://www.blocquebecois.org>; <http://www.ndp.ca>; <http://www.pcparty.ca>.

[246] See for example People for Education, online: <http://www.peopleforeducation.com>; National Citizens' Coalition, <http://www.morefreedom.org>. A number of U.S. sites are at <http://www.grassroots.com>. International groups are online at the Association of Progressive Communications, <http://www.apc.org>.

[247] Martin Stone, "Bush Dead Last in Online Fundraising", E-Commerce Times, February 7, 2000, online: <http://www.ecommercetimes.com/perl/story/2441.html>.

[248] See for example <http://www.ethepeople.com>, "America's Interactive Town Hall".

[249] See for example Ontario's consultation on private sector privacy legislation, updated to August 2002, online: <http://www.cbs.gov.on.ca/mcbs/english/56HK6V.htm>.

[250] See online: <http://www.22minutes.com/featuredclip.php>.

[251] Singapore in July 2001 asked a political commentary site to register as a political organization under its broadcasting statute. See Declan McCullagh, "Singapore orders political Web sites to register with government" (July 2001), online: <http://www.politechbot.com/p-02257.html>.

[252] See for example Voteswap, online: <http://voteswap.com>.

[253] Of course, it did not work out, either for Gore or for Nader.

[254] Duncan Campbell, "Vote-trading Web sites close", The Guardian, November 2, 2000, online: <http://www.guardian.co.uk/internetnews/story/0,7369,391576,00.html>.

[255] American Civil Liberties Union, "ACLU Seeks Permanent Court Order on Issue of Online Voter Matching", November 27, 2000, online: <http://www.aclu.org/news/2000/n112700.html>.

[256] Such deals raise similar legal issues to B2B, business-to-business, electronic commerce.

[257] The virtual communities referred to in the discussion of regulation, *supra*, text accompanying note 133, may play a political role too, without becoming parties in the traditional sense.

[258] J. Gregory, "Law Reform and the Internet" (2000), online: <http://www.euclid.ca/lawreform.html>.

[259] See D. Tapscott and D. Agnew, "Governance in the Digital Economy" (1999), online: <http://www.imf.org/external/pubs/ft/fandd/1999/12/tapscott.htm>, and the "Governance in the digital economy Web site", online: <http://egov.actnet.com/public>.

[260] This discussion draws to some extent on the exploratory work done by the Crossing the Boundaries project led by Reg Alcock, M.P., online: <http://www.crossingboundaries.ca>. See also that project's principal study paper to date: H. Schachter, "Crossing Boundaries: Privacy, Policy and Information Technology" (1999), online: <http://www.ipaciapc.ca/english/research/IPAC-5.pdf>.

[261] Both areas were found after litigation to be subject to federal control. This article does not, however, suggest that the problems discussed are soluble by federal regulation of Internet communications.

[262] Ontario Business Connects, "Anchoring new Value Systems through Infrastructure", (December 1999), online: <http://www.cbs.gov.on.ca/pdf/discuss3e.pdf>, at p. 2.

[263] For one example among many, see HumanRightsTech.org, "We leverage information technology to assist and encourage grass-roots anti-poverty initiatives.", online: <http://www.humanrightstech.org>.

[264] See Henry H. Perritt, Jr., "The Internet and Public International Law", (2000) 88 Ky.L.R. 885, at 894.

[265] For example, see these Internet sites, online: International Campaign to Ban Landmines, <http://www.icbl.org>; Anti-globalization movements: <http://www.globalization.about.com/cs/antiglobalization>; Lawyers' Committee on Human Rights, supporting the ICC: <http://www.lchr.org/feature/50th/main.htm>.

[266] See <http://www.bcli.org/pages/database/index2.html> for the database on law reform projects in the English-speaking world, originally assembled by its predecessor, the British Columbia Law Reform Commission. This used to be available on diskette on request; it is now available any time, anywhere.

[267] For more examples, see my article, "Foreign Influences on Canada's Electronic Commerce Legislation", <http://www.euclid.ca/foreign.html>.

[268] Dean Perritt's study at *supra* note 264 refers to Bhutan and Ukraine as examples.

[269] Henry H. Perritt, Jr. "Cyberspace and State Sovereignty", (1997) 3 J.Int'l Legal Stud. 155, online at <http://www.kentlaw.edu/perritt/professorperritt/jilspub.html>. See also <http://pbosnia.kentlaw.edu/roltt/> for "Rule of Law through Technology".

[270] Margaret Knight, "Pioneers of the Internet", Rensselaer. Mag, (September 2000), online: <http://www.rpi.edu/dept/NewsComm/Magazine/Sep00/Pioneers.html>.

[271] Though data bases and computer processing other than communications with other computers would not be affected by non-compliance with Internet protocols.

[272] (Harvard: Cambridge, 1999). Details online: <http://www.code-is-law.org>. See also <http://www.lessig.org> for links to articles, speeches and other documents by and about Professor Lessig.

[273] *Supra* note 117 and accompanying text.

[274] *Patent Act*, R.S.C. 1985, c. P-4.

[275] *Trade-marks Act*, R.S.C. 1985, c. T-13.

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

[277] *Ibid.* at s. 6. Some countries have extended the protection to life plus 70 years.

[278] *Ibid.* at s. 29 (fair dealing), s. 29.3 (copying by academic institution covering costs only).

[279] *Supra* note 118.

[280] See text accompanying note 122.

[281] *Supra* note 120 at s. 1201.

[282] See for example the Digital Future Coalition's news release for October 27, 2000, at <http://www.dfc.org/dfc1/Active_Issues/graphic/1201_release.html>.

[283] See for example David Post, "What Larry Doesn't Get" (2000) 52 *Stanford L.R.* 1439. <http://www.temple.edu/lawschool/dpost/Code.pdf> and "Governing Cyberspace: Where is Thomas Jefferson When We Need Him?" <http://www.temple.edu/lawschool/dpost/icann/comment1.html.>

[284] See online: <http://www.icann.org>.

[285] ICANN Fact Sheet, online: <http://www.icann.org/general/fact-sheet.htm>.

[286] ICANN At-Large Membership Study Committee, "At-Large Membership Study Committee Discussion Paper #1", July 2001, online: <http://www.atlargestudy.org/DiscussionPaper1.shtml>.

[287] See ICANN Watch, online: <http://www.ICANNwatch.org>, Michael Froomkin's collection of comments, online: <http://personal.law.miami.edu/~amf/> (accessed July 23, 2001), and the summary of concerns about process in creating new top-level domain names, written on behalf of a number of liberal organizations (January 2001), online: <http://www.internetdemocracyproject.org/DoClt1.htm> (accessed July 23, 2001).

[288] The Board is listed online: <http://www.icann.org/general/abouticann.htm#BoardofDirectors> (accessed July 23, 2001). Professor Lessig was a candidate in a recent election, but was not elected. See <http://www.lessig.org>.

[289] <http://www.cira.ca>.

[290] <http://www.cira.ca/official-doc/8.RPPG_00015EN.pdf>.

[291] <http://www.cira.ca/en/cat_Dpr.html>.

[292] <http://www.wipo.org>, *supra*, text accompanying note 30.

[293] However, some WIPO dispute resolution awards have been appealed to courts, particularly in the United States, under general laws of arbitration permitting such recourse or on procedural reviews. The relationship between the awards and the powers of the court over the disputes is not yet clear.

[294] The House Committee on Energy and Commerce's Subcommittee on Telecommunications and the Internet held hearings in February 2001 on ICANN's creation of new top-level domain names. Online: <http://energycommerce.house.gov/107/hearings/02082001Hearing37/hearing.htm>. The Senate Commerce Committee considered ICANN governance on June 12, 2002. Proceedings are online: <http://commerce.senate.gov/hearings/hearings0202.htm>.

[295] The Secretary of Commerce reviewed a contract between ICANN and Verisign about the administration of the *.com* and *.org* domains. <http://energycommerce.house.gov/107/letters/03302001_150.htm>.

[296] Michael Froomkin, "Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution", (2000) 50 Duke L.J. 17, online: <http://www.law.miami.edu/~froomkin/articles/icann-main.htm>.

[297] <http://www.isoc.org>.

[298] <http://www.ietf.org>.

[299] <http://www.irtf.org>.

[300] <http://www.itu.int>. This body was formerly known as the International Telegraph Union; since the 19th century it has been governing communications between nations by wire and later by wireless.

[301] <http://www.iso.ch>.

[302] See John D. Gregory, "Solving Legal Issues in Electronic Government: Authority and Authentication", (2002), 1 CJLT 1.

[303] <http://www.nist.gov/public_affairs/factsheet/ecommerce.htm>.

[304] <http://www.ansi.org>.

[305] <http://www.x9.org>.

[306] American Bar Association, "Digital Signature Guidelines", (Chicago, ABA, 1997) online: <http://www.abanet.org/scitech/ec/isc/dsg-free.html>.

[307] American Bar Association, "PKI Assessment Guidelines (PAG)", detailed draft guidelines for evaluating PKI systems, online: <http://www.abanet.org/scitech/ec/isc/pag/pag.html>.

[308] <http://www.ict.etsi.org>.

[309] <http://www.ict.etsi.org/eessi/EESSI-homepage.htm>.

[310] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, online: search at <http://europa.eu.int/eur-lex/en/search/search_lif.html> for Directive, year 1999, document 93.

[311] <http://www.scc.ca>.

[312] <http://w3.pwgsc.gc.ca/cgsb/text/eng-e.html>.

[313] CAN/CGSB-72.11-93, described online: <http://www.pwgsc.gc.ca/cgsb/catalogue/specs/072/072_011-e.html>. The *Uniform Electronic Evidence Act*, [1998] Proceedings of the Uniform Law Conference of Canada 164, online: <http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2>, specifically authorizes courts to consider the degree to which electronic records comply with applicable standards of record integrity.

[314] <http://tsacc.ic.gc.ca>.

[315] <http://www.e-com.ic.gc.ca>.

[316] *Supra* note 103, notably Chapter IV, Division 1, s. 67.

[317] <http://www.criq.qc.ca/bnq/english/index.html> (accessed July 23, 2001).

[318] *Supra*, text accompanying note 35.