BORDEN
LADNER
GERVAIS

Internet Law Handbook

Bradley J. Freedman
Robert J. C. Deane

Lawyers – Patent & Trademark Agents

INTERNET LAW HANDBOOK

Bradley J. Freedman
Robert J.C. Deane

Borden Ladner Gervais LLP

Published in 2001 by Borden Ladner Gervais LLP.

Table of Contents

1

INTRODUCTION

The Internet and related technologies are removing barriers to markets, facilitating new business models, and fostering a global marketplace. Canadian businesses are embracing the advantages of electronic commerce for business-to-business and business-to-consumer transactions.

New technologies present substantial opportunities, but they also present legal and business risks. Consider the following:

- the Internet and related technologies present significant risks regarding the use and protection of copyright-protected works and trade-marks;
- electronic communications can be used to create contracts, but to be valid and enforceable those contracts must comply with laws regarding electronic commerce, electronic evidence and Internet consumer protection;
- the nature of Web sites and other Internet communications, including the use of links, multimedia content, and other technologies, presents risks of inadvertently violating advertising laws;
- Web site development and hosting may present numerous project management and outsourcing challenges;
- the collection, use and disclosure of personal information present significant privacy and confidentiality issues;
- modern communications systems present significant business and legal risks; and

- the Internet presents considerable challenges for securities market participants seeking to ensure that their Internet activities comply with applicable laws, and for regulators seeking to protect investors and the integrity of capital markets.

Some of these legal and business risks have been addressed by lawmakers through the enactment of laws regarding electronic commerce, electronic evidence, Internet consumer protection, and Internet trade-mark infringement. Regulators have also issued helpful guidance regarding the application of general laws to Internet activities. Other risks may be addressed by private contracting – Web site development and hosting agreements, Web site use agreements, electronic transaction agreements, privacy policies, and communications system policies – and prudent risk management. Residual risks may be addressed by insurance.

This Handbook provides a brief discussion of some of the legal challenges presented by the Internet and related technologies, and some of the ways in which resulting business and legal risks may be addressed. While we hope that you find this Handbook useful, the information in this Handbook is of a general nature, and should not be regarded as legal advice. Internet law is complex and developing rapidly, and must be considered in the circumstances of each individual transaction, case or issue.

Organizations engaged in Internet activities should regularly review their business strategies and risk management practices to ensure that they comply with evolving laws and regulatory guidance, and are consistent with current business and technical best practices. They should also obtain legal advice specific to their circumstances.

Bradley J. Freedman and Robert J.C. Deane
Borden Ladner Gervais LLP
Vancouver, British Columbia, Canada
bfreedman@blgcanada.com
rdeane@blgcanada.com

2

COPYRIGHT AND THE INTERNET

The Internet and related technologies present particular difficulties in protecting copyright due to the high quality of digital copies, the low cost of digital reproduction and distribution, the ability of infringers to act anonymously, and the prevalence of users who either are unaware of applicable copyright laws or choose to ignore them. However, there are a number of measures that may be taken to preserve and protect copyright on the Internet and minimize the risk of infringing the rights of others.

Copyright Basics

Copyright comprises the exclusive right to produce or reproduce a work or any substantial part of it in any material form, and the associated right to prevent others from doing so. In essence, the owner of copyright in a work has a time-limited, exclusive right to almost all commercially valuable uses of the work. Copyright subsists in every original literary (including computer software), dramatic, musical and artistic work, as well as in performances, sound recordings and broadcasts. To be protected by copyright, a work must be original in the sense that it originated from its author, but there is no requirement that the work be novel or its subject matter have merit. Copyright protects only the form of expression, but not the underlying ideas or facts.

Copyright infringement occurs when a person does something, without the consent of the copyright owner, that only the copyright owner has the right to do, such as performing, reproducing or publishing a work, or authorizing another person to do such an act.

Generally, the creator of a work (the person who actually wrote, drew, composed or produced the work) is considered to be the owner of the copyright in the work. However, there are different rules for ownership of copyright in works created by employees and independent contractors. If a work is created by an employee in the course of their employment, then copyright in the work is owned by the employer unless there is an agreement to the contrary. To avoid uncertainty, employment agreements should specifically address copyright ownership issues. If a work is created by an independent contractor (such as a consultant or freelancer), then in most cases copyright in the work is owned by the contractor and not the person who engaged and paid the contractor to create the work. Accordingly, anyone engaging an independent contractor to create a work should obtain a written assignment of the copyright. Failure to do so may limit the ability of the person who paid for the work to use the work in the future.

Common Internet Uses

Common uses of the Internet – posting, browsing, transmitting, downloading, and caching – may give rise to copyright infringement liability. Many separate, copyright-protected works may be involved in an Internet communication, and the rights of the owners of each of those works may be infringed by Internet use. Further, a single Internet use of a work may infringe various aspects of copyright.

Each kind of Internet activity must be examined individually in its particular circumstances to determine whether there has been an infringement of a particular right, whether there is a defence to liability, and who bears

liability. The following is a brief summary of some copyright law issues presented by common uses of the Internet:

- **Browsing:** Browsing the Internet requires the user's computer to create a temporary copy of the accessed Web site in the computer's short term memory (RAM) and often creates a more permanent copy on the computer hard drive.
- **Caching:** Caching is the creation of copies of material in a computer memory to facilitate quick access to the work. Internet service providers and other Internet intermediaries often engage in caching to provide faster access to popular Internet materials. Web browser software also caches copies of Internet materials in a "Temporary Internet Files" directory to accelerate system performance. Both forms of caching involve copying and reproduction of the stored materials.
- **Downloading:** Downloading data from the Internet involves making a copy of the downloaded information in the user's computer hard drive or random access memory.
- **Posting and Transmission:** The posting of a work on a Web site involves making a copy of the work, authorizing the communication of the work to the public, and authorizing the copying and reproduction inherent in the browsing and downloading of the work.
- **Linking:** Links between Web sites are the central feature of the Web's user interface and provide the easy, point-and-click method of navigating from one Web site to another. No copying is involved in providing a link, because the link merely causes the user to connect to the particular Web page of the original author and is analogous to using a library card index to locate particular items, albeit more efficiently. Nevertheless, creating a link may constitute a communication of the linked work to the public or the authorization of such communication. A Web site link may also be designated by copyright-protected text, icons, graphics or other works.

- **Framing:** Framing is a technique that divides a computer screen into multiple windows, each of which can display content from the same or different Web sites. The effect is similar to the picture-in-picture feature on television sets. Framing can result in the apparently seamless integration of two or more Web sites, which to the user may appear to originate from a single source. Framing can also display advertising or other information around windows displaying content from other Web sites. Like linking, framing does not result in the copying of the framed content. The framing technique simply directs users' computers to obtain content from another Web site or Internet resource. Nevertheless, framing may result in the combination of content and the creation of a new, composite work or compilation. It may also authorize the communication of the framed work to the public.

At least one Canadian court has held that a person who posts works to publicly accessible Internet sites grants an implied licence to Internet users to use the works in a manner consistent with ordinary Internet practice. The existence and scope of the implied licence will depend upon the particular circumstances, but would likely include the right to browse and review the works. The defence of implied licence is subject to at least three significant limitations: (a) an implied licence does not cover acts that are not part of the reasonable and customary use of works posted on the Internet, such as further reproduction and public distribution; (b) an implied licence is subject to notice of contrary use restrictions, such as those often found in Web site use agreements; and (c) an implied licence is effective only to the extent the person purporting to grant the licence owns copyright in the work.

The Canadian federal government is considering amending the *Copyright Act* to specifically address Internet copyright liability issues. In the meantime, Internet users should ensure that they have the right to post works on the Internet, and that information accessed or obtained through the Internet

is used in a lawful manner consistent with general copyright laws and contractual use restrictions.

Digital Distribution Rights

A licence to publish a work in one medium does not necessarily imply a right to publish the work in other media. Most agreements between authors and publishers now expressly provide for electronic and new media reproduction and distribution rights, including CD-ROM compilations and Internet distributions. Where agreements are silent on that issue, the publisher's right to create CD-ROM compilations and digital distributions will be determined by the agreement terms and applicable copyright laws, which generally provide that authors retain control of the copying and dissemination of their work through different media.

Internet Intermediary Liability

Most Internet users access and use the Internet through the facilities of an Internet Service Provider (ISP) or other Internet intermediary. In providing their services, Internet intermediaries transmit, copy, cache, store, and index materials used by others. Copyright holders have frequently sought to impose copyright infringement liability upon Internet intermediaries for practical reasons – they are easier to locate than individual Internet users (who are often located in a foreign jurisdiction or take other measures to avoid detection), they have the means to satisfy a money damages award, and the risk of liability may deter them from facilitating infringement by others.

In the United States, courts have imposed liability for copyright infringement on Internet intermediaries that play an active role in infringing activities. Internet intermediaries that play a passive role and only provide the means by which others engage in infringing activities have not been held liable for copyright infringement, unless they have knowledge of the spe-

cific infringing activity and the means to stop it. A similar approach has been taken by the Canadian Copyright Board.

The U.S. *Digital Millennium Copyright Act* ("*DMCA*") now specifically provides that an Internet intermediary that plays a passive role in the impugned activity and satisfies certain other criteria may be protected from copyright infringement liability arising from its routing, caching, storage and linking activities. There is no Internet-specific legislation in Canada providing Internet intermediaries with protection from copyright liability, but the Canadian Copyright Board has held that certain general exemptions from copyright infringement liability provided by the *Copyright Act* may have a similar effect. The Canadian government is considering amending the *Copyright Act* to specifically address Internet intermediary liability issues.

Circumvention of Copyright Protection Systems

The World Intellectual Property Organization *Copyright Treaty 1996* requires contracting countries to provide adequate legal protection and effective legal remedies against the circumvention of technological measures used to protect copyright. The U.S. *DMCA* complies with this requirement by: (a) prohibiting the circumvention of a technological protection measure put in place by the copyright owner; and (b) prohibiting the manufacture or distribution of certain technologies, products and services used to defeat technological measures controlling access. The *DMCA* provides a number of exceptions to the prohibition regarding circumvention and circumvention devices, including exceptions for reverse engineering; law enforcement and intelligence activities; encryption research; security testing; parental supervision of minors; the protection of personal information; non-profit libraries, archives, and educational institutions; and certain analogue devices and technologies. The *DMCA* provides civil remedies (injunctions, damages, costs and attorney's fees) and criminal penalties for violations of the copyright protection system provisions.

There are no Canadian laws specifically relating to the circumvention of copyright protection systems. However, the Canadian government is considering legislation prohibiting the circumvention of technological measures used to protect copyright.

Database Protection

Traditionally, copyright law has protected only forms of expression, and not the underlying ideas or facts. This has resulted in little or no protection for databases, the value of which lies primarily in the compiled factual information. This issue has been address by the European Union through a *Directive on the Legal Protection of Databases*, which requires EU member states to implement laws to create a *sui generis* property right in the content of a database in which there has been a "substantial investment", qualitatively or quantitatively, in obtaining, verifying, or presenting the content. The *sui generis* database right prohibits acts of "extraction" and "re-utilization" of the whole or a substantial part, evaluated qualitatively or quantitatively, of the contents of the database. The right also prohibits "repeated and systematic" extraction or re-utilization of insubstantial parts of the database contents if such acts conflict with the normal exploitation of the database or unreasonably prejudice the legitimate interests of the database owner. Neither Canada nor the United States have enacted database protection laws, but both are considering whether to do so.

Jurisdiction Issues

The trans-jurisdictional nature of the Internet may present liability risks arising from differences in copyright laws among different states. For example, communications originating in Canada and lawful under Canadian law may be unlawful in other countries where the communications are received. Similarly, the divisible nature of copyright may present liability risks where ownership of copyright in a particular work is shared among persons in different countries. For example, if different persons own the

Canadian and U.S. rights to a work, they may not be permitted to distribute the work over the Internet to residents of the other country.

Risk Management

The following are some measures that may be taken to preserve and protect copyright on the Internet and minimize the risk of infringing the rights of others:

- Copyright owners should register their copyright and ensure that all materials bear appropriate copyright notices.
- Licence agreements should be obtained for all content published and distributed on the Internet.
- Technological measures, such as encryption, tagging, fingerprinting and other anti-copying devices, may be used to prevent unauthorized use of materials or to assist in the detection and enforcement of copyright infringement.
- Internet-related agreements, including Web hosting and Web site use agreements, should expressly indicate the permitted and prohibited uses of the Web site content and provide a procedure for responding to claims of copyright infringement and other misconduct.

3

TRADE-MARKS AND THE INTERNET

The Internet presents significant challenges and risks regarding the use and protection of trade-marks. Trade-marks may be infringed by Web site domain names and content, as well as by common Internet activities such as linking and framing. However, there are a number of measures that may be taken to preserve and protect trade-marks on the Internet, and to minimize the risk of infringing the rights of others.

Trade-mark Basics

A trade-mark is a distinctive mark used in connection with goods or services to identify the source of those goods or services and to distinguish them from the goods or services of others. A trade-mark may take many forms including a word, phrase, design or logo, a set of numbers, letters or symbols, a colour, a shape, or a combination of any of those elements.

To be protected, a trade-mark must distinguish a trader's goods and services from the goods and services of others. The ability to distinguish, known as "distinctiveness", is the key requirement of a protectable trade-mark. Distinctiveness may be inherent or may be acquired through use. Distinctiveness may be lost as a consequence of the unauthorized or uncontrolled use of the same or similar trade-marks by others.

Trade-mark owners can prevent others from using the same or confusingly similar trade-marks. An impermissible likelihood of confusion exists when ordinary consumers would likely believe that the goods or services associated with the original and challenged trade-marks are from the same source, or that the goods and services associated with the challenged trade-mark are in some way approved, authorized, or endorsed by the owner of the original trade-mark. Trade-mark owners can also prevent others from using their trade-mark in a manner that depreciates the goodwill associated with the mark.

Domain Names

Domain names are the alpha-numeric addresses of sites on the Internet. Domain names are the simplest way to locate Web sites. Indeed, it is common for Internet users who do not know a desired Web site domain name to simply guess the domain name by using the Web site owner's trade-mark and a domain suffix, in the form *www.[trade-mark].com*. Domain names often incorporate key trade-marks and may be valuable assets.

Domain names are administered by various approved domain name registrars, and are generally issued on a first-come-first-served basis upon payment of a registration fee. However, like corporate names, the registration and use of Web site domain names are subject to applicable trade-mark laws.

The most well-known domain name disputes have involved the opportunistic practice of pre-emptively registering domain names that incorporate well-known trade-marks or trade-names and then offering to sell them to the highest bidder (usually the party to whom the incorporated trade-mark properly belongs). Courts have generally held that this practice, commonly known as "cybersquatting", constitutes unlawful trade-mark use because it is likely to confuse or mislead Internet users, or constitutes a misrepresen-

tation regarding the approval, authorization, or endorsement of the trade-mark owner.

Currently, there is no Canadian legislation that deals specifically with cybersquatting. Nevertheless, in many cases general trade-mark law may provide an adequate remedy against cybersquatting. In addition, certain disputes over alleged bad faith registration and use of *.com*, *.net*, *.org*, *.biz* and *.info* domain names may be resolved pursuant to the *Uniform Domain Name Dispute Resolution Policy* (the "*Policy*") promulgated by the Internet Corporation for Assigned Names and Numbers ("ICANN"). The *Policy* is intended to be an efficient and cost-effective procedure for resolving the most clear-cut cybersquatting disputes. Under the *Policy*, disputes are determined by an administrative panel established by an approved dispute-resolution service provider. In most cases, hearings are based on written submissions and documentary evidence, and disputes are generally resolved within 45 days. Administrative panels may order that a domain name registration be cancelled or transferred to a complainant that successfully proves: (a) the domain name is identical or confusingly similar to the complainant's trade-mark; (b) the registrant has no rights or legitimate interests in the domain name; and (c) the domain name was registered and is being used in bad faith

The U.S. *Anticybersquatting Consumer Protection Act* ("*ACPA*") was enacted to specifically address cybersquatting. The *ACPA* protects owners of famous or distinctive trade-marks by providing a civil cause of action against any person who in bad faith registers, traffics in, or uses a domain name that is identical or confusingly similar to a distinctive mark or name, or is identical to, confusingly similar to, or dilutive of a famous mark. The *ACPA* also protects individual rights of privacy and publicity by providing civil remedies against persons who register a domain name consisting of another living person's name, or a substantially and confusingly similar name, with the specific intent to profit by selling the domain name to that person or

any other person. The *ACPA* does not apply to other forms of trade-mark misuse on the Internet. The *ACPA* may provide significant benefits for trade-mark owners whose marks have been used in bad faith in domain names registered by others. Canadian businesses with a presence in the United States or that are dealing with domain name registrants located in the United States may therefore consider bringing proceedings in U.S. courts to invoke the *ACPA*.

Not all conflicts between domain names and trade-marks constitute unlawful trade-mark use. In particular, conflicts may arise between two legitimate trade-mark owners, both wishing to use their marks or names on the Internet. Trade-mark law is ill-suited to resolving such conflicts. In those cases, the first legitimate user to register the domain name in good faith will likely prevail if: (a) the use is not likely to confuse or mislead Internet users; or (b) the domain name does not constitute a trade-mark use in a jurisdiction in which another trade-mark owner has prior rights.

Misleading Meta-Tags and Hidden Text

Web sites may incorporate meta-tags (hidden codes that provide key word descriptions of Web sites) and hidden text that contain names and trade-marks belonging to competitors or that otherwise have no legitimate connection with the Web site to cause search engines to reference the Web site in response to queries regarding those descriptions, names or marks. Misleading meta-tags and hidden text may constitute trade-mark infringement and misuse if they create a likelihood of confusion or constitute a misrepresentation.

Links

Links between Web sites may infringe trade-mark rights if they are designated by icons that incorporate trade-marks, or if they falsely suggest the sponsorship, approval, or affiliation of the linked site.

Framing

Framing is a technique that divides a computer screen into multiple windows, each of which can display content from the same or different Web sites. Framing may result in the trade-marks displayed on one Web site being used in association with the goods or services sold or advertised on another site, which may constitute trade-mark infringement.

Criticism or Parody Web Sites

Trade-marks may sometimes be used in Web site domain names or content to facilitate comment, criticism, or parody of the trade-mark owner. Registering domain names in the form *www.[trademark]sucks.com* for Web sites that provide a forum for critical commentary is part of the Internet phenomenon known as "cybergriping". Where the use of trade-marks in association with critical Web sites is likely to confuse or mislead, there may be trade-mark infringement or passing-off. However, recent court decisions have attempted to balance trade-mark rights and free speech rights, with the result that many criticism or parody Web sites have been held not to infringe trade-mark rights.

Web Site Content

Trade-marks may be infringed by Web site content. In determining whether Web site content infringes trade-mark rights, the similarity of the marks, the similarity of the goods or services, and the simultaneous use of the Web as a marketing channel are important considerations.

Jurisdiction Issues

The global nature of the Internet presents the risk that Internet trade-mark use that is lawful in the Web site owner's jurisdiction may violate foreign laws or trade-mark rights. When those issues arise, determining the laws that govern the Internet conduct and the courts or regulators that have jurisdiction over the conduct may be highly significant.

As a general rule, in private law matters, the existence of real and substantial connections (or "minimum contacts" in the United States) between a state and the offending activity is central to determining whether the state's courts have jurisdiction. American and Canadian courts have adopted a sliding scale approach based upon traditional legal principles. They have not asserted jurisdiction over foreign owners of "passive" Web sites (those that do not have active contact with residents of their jurisdiction), but have generally asserted jurisdiction over foreign owners of "active" Web sites used to communicate and engage in commerce with residents of the court's jurisdiction. In cases involving cybersquatting, U.S. courts have tended to assert jurisdiction on the basis that the defendant's wrongful activities were directed to the court's jurisdiction and caused the trade-mark owner harm in that jurisdiction.

Risk Management

The following are some measures that may be taken to preserve and protect trade-marks on the Internet and minimize the risk of infringing the rights of others:

- **Mark Selection Strategies:** Conduct appropriate trade-mark searches and other due diligence before commencing to use trade-marks on the Internet and before registering and using domain names.
- **Register and Use Domain Names as Trade-marks:** To the extent possible, use and register domain names as trade-marks. Use as merely a Web site address is likely not sufficient to support a claim of trade-mark rights. To satisfy Canadian trade-mark law requirements, domain names should be used as source identifiers for wares and services and should be marked on wares and their packaging and used in advertisements for services on the Web site and elsewhere.

- **Register and Use Trade-marks as Domain Names:** To the extent possible, trade-marks should be registered and used as domain names. Registrations should be made in all available generic domains and important country domains. Registrations should also be made for reasonable variations of the marks (including common incorrect spellings). Consideration should also be given to the registration of likely critical domain names, such as *[trade-mark]sucks.com*.

- **Declare Trade-mark Rights:** All trade-mark uses should include an appropriate trade-mark designation: the symbols "TM", "Registered Trade-mark" or "Reg'd T.M.". Trade-mark owners should declare their trade-mark rights on their Web sites and in enforceable Web site use agreements.

- **Trade-mark Use Agreements:** Users of other persons' trade-marks should ensure that Internet trade-mark use is authorized by a trade-mark licence. Conversely, trade-mark owners should not allow their marks to be used by others without appropriate licence agreements and trade-mark declarations. Unauthorized or uncontrolled trade-mark use by others may impair the distinctiveness of the mark and may result in a loss of trade-mark rights.

- **Web Site Jurisdiction Measures:** Measures should be taken to reduce the risk of foreign courts and regulators asserting jurisdiction over Web site conduct, and the risk of liability for infringing foreign trade-marks. Domain names should be registered with local domain name registrars. Web sites should have appropriate jurisdiction disclaimers and Web site gate pages that restrict Web site access to users who reside in particular jurisdictions. Also, Web site use agreements should contain provisions stipulating the permissible users of the Web site, the laws that apply to the Web site and its use, and the courts that have jurisdiction over disputes regarding the Web site and related matters.

- **Monitor Internet Trade-mark Use:** On a regular basis, the Internet (including Internet domain name registries) should be searched to detect unauthorized trade-mark use. Commercial trade-mark search services may be engaged to provide this service.
- **Trade-mark Rights Enforcement:** Trade-mark rights should be enforced in a reasonable and practical manner. Not every similar domain name or trade-mark use will be infringing. Inappropriately heavy handed tactics can be counter-productive and result in detrimental adverse publicity. When dealing with cybersquatters, Canadian Web site owners should consider commencing U.S. litigation to invoke helpful U.S. laws. Canadians accused of Internet trade-mark misuse should consider commencing proceedings in Canada for a declaration that their activities are lawful.
- **Cooperative Use.** Competing legitimate users of the same trade-mark may consider establishing a joint Web site portal that uses the shared trade-mark and allows users to select the Web site they wish to access. For example, see *www.scrabble.com*.

4

ELECTRONIC CONTRACTS

Electronic contracts present specific challenges to traditional contract law principles, including rules regarding contract formation (offer and acceptance), statutory formalities (writing, signature, and delivery requirements) and enforcement (evidentiary issues). Canadian lawmakers have addressed those challenges by enacting electronic commerce laws and electronic evidence laws. Canadian courts have also confirmed that contracts formed over the Internet may be valid and binding.

The Legal Effectiveness of Electronic Communications

For most kinds of contracts, Canadian law does not require any particular formalities, such as writing, signature, and delivery. Courts have held that agreements formed by email or by users clicking an "I Agree" icon on a Web site can be valid and enforceable. Nevertheless, certain contracts must comply with required formalities to be valid and enforceable. Lawmakers in Canada and elsewhere have enacted electronic commerce laws that prescribe how electronic communications may be used to satisfy contract formality requirements.

Generally, electronic commerce laws make other more general laws equally applicable to paper-based and functionally equivalent electronic communications, and provide some basic rules for electronic contracts and com-

munications. Canadian electronic commerce laws vary from province to province, but most provide as follows:

- Information shall not be denied legal effect or enforceability solely because it is in electronic form, and a contract shall not be denied legal effect or enforceability solely because an electronic document was used in its formation. There are exceptions for certain kinds of documents and contracts, including wills, powers of attorney, negotiable instruments, and documents that create or transfer interests in land.
- Persons are not obliged to use or accept information in electronic form without their express or implied consent.
- Unless the parties agree otherwise, an offer or acceptance or any other matter that is material to the formation or operation of a contract may be expressed by means of an electronic document or by an action in electronic form, including touching or clicking on an appropriately designated icon on a computer screen, or otherwise communicating electronically.
- Contracts may be made by the interaction of an electronic agent and a natural person, or by the interaction of electronic agents. An "electronic agent" is defined as a computer program or any electronic means used to initiate an action or to respond to electronic documents or actions in whole or in part without review by a natural person. Generally, a natural person contracting with an electronic agent must be permitted to correct mistakes without incurring contractual liability.
- A legal requirement that information be in writing is satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference.
- In most instances, a legal requirement for a signature is satisfied by an electronic signature if: (a) it is reliable for the purpose of identifying the person; and (b) the association of the electronic signature with the relevant electronic document is reliable for the purpose for which the electronic

document was made. An "electronic signature" is defined as information in electronic form that a person has created or adopted to sign a document and that is in, attached to or associated with the document.

- A legal requirement that written information be provided to another person is satisfied by the provision of an electronic document that is accessible by the other person and capable of being retained by that person for subsequent reference.
- A legal requirement that a document be retained is satisfied by the retention of an electronic document if: (a) it is retained in the format in which it was made, sent or received, or in a format that does not materially change the information contained in the document; (b) it will be accessible so as to be usable for subsequent reference by authorized persons; and (c) if the document was transmitted, information that identifies its origin and destination, and the date and time when it was sent or received, is also retained.
- An electronic document is not capable of being retained if the person delivering it inhibits the printing or storage of the document by the recipient.
- A legal requirement that a person present or retain an original document is satisfied by an electronic document if: (a) there is a reliable assurance as to the integrity of the information in the document from the time it was originally made; and (b) it is accessible and capable of being retained by the person to whom it is given for subsequent reference.
- Unless the parties otherwise agree, a message is deemed to be sent when it enters an information system outside the control of the sender. A message is presumed to be received when it enters an information system designated or used by the recipient and is capable of being retrieved and processed by the recipient. Unless the parties otherwise agree, electronic

documents are deemed to be sent from the originator's place of business and are deemed to be received at the recipient's place of business.

Most Canadian electronic commerce laws are basic laws that stipulate fundamental legal rules and prescribe minimum legal requirements. In some circumstances, prudence will dictate the use of technologies or practices that exceed basic legal requirements. For example, although there is generally no legal requirement for most commercial agreements to be in writing or signed, most commercial agreements are memorialized in a written document signed by the parties. Similarly, over time, businesses will likely develop commercially acceptable electronic practices that supplement statutory basic rules.

Quebec's electronic commerce law is different from the laws of the other Canadian provinces. It provides fewer rules for electronic contracting, and addresses other matters such as regulations regarding secure electronic signatures and the use of biometrics.

Electronic Standard Form Contracts

Like most conventional consumer transactions, electronic transactions will usually involve non-negotiable, take-it-or-leave-it standard form contracts. Applying conventional legal principles, courts in Canada and the United States have held that standard form electronic contracts are valid and enforceable if the user accepts the contract explicitly or by unambiguous conduct.

Standard form electronic contracts are often implemented as "click-through" agreements. Users are presented with a gateway page (also known as a "click-through" page) and the terms of the agreement, and are required to indicate their acceptance or rejection of the agreement by clicking an "I Agree" icon. Only users who click the icon are allowed to proceed with the transaction. Courts have generally held click-through agreements to be valid.

Standard form electronic contracts may also be implemented as "notice-and-acceptance-by-conduct" agreements. Users are given notice that by engaging in certain conduct (such as using a Web site or downloading software) they are deemed to have accepted the agreement. Courts have held that notice-and-acceptance-by-conduct agreements may be valid, but only if the notice is sufficiently prominent to be seen by users and fairly warns users that their unambiguous conduct will result in acceptance of the contract terms.

As with conventional, unsigned standard form contracts, unusual or onerous terms will not be enforceable unless they have been reasonably drawn to the user's attention. It is also important to note that Internet consumer protection laws generally require that all contract terms be presented to the consumer in a conspicuous manner before the transaction is concluded.

Contract Formation Risks

Electronic contracts present various contract formation risks relating to: (a) contractual offers and acceptances and contract formation timing; (b) the identity, capacity and authority of contracting parties; and (c) the legal effectiveness of automated contracting systems. Some of those risks are addressed by electronic commerce laws. Other risks may be addressed by the contracting parties carefully stipulating the intended terms and effect of their communications and establishing their own contract formation rules.

Where the parties expect to engage in numerous electronic transactions, they may wish to first enter into a general agreement that establishes contract formation rules for subsequent transactions. If multiple transactions are not intended, the parties may stipulate contract formation rules in their offers and counter-offers. The following are some of the more significant contract formation rules that should be addressed in either case.

- **Offer or Solicitation:** Web site advertisements should indicate whether they are offers to sell capable of acceptance, or merely solicitations of offers to purchase.
- **Standard Terms:** Internet vendors may wish to structure Web site transactions so that purchase orders must include the vendor's standard terms and conditions.
- **Order Cancellation:** Electronic offers should state the circumstances, if any, in which they may be revoked by the offeror and the manner in which the revocation must be effected.
- **Automated Responses:** Automated responses intended only to acknowledge receipt of contractual offers should state that they do not constitute an acceptance creating a contract.
- **Acceptances:** Electronic offers should state the exclusive manner in which an acceptance may be made and communicated.
- **Amendments:** Standard form contracts should be implemented in a way that prevents amendments or additions to contractual terms.
- **Contract Formation Timing:** Contracting parties should agree upon the circumstances in which electronic communications will be considered to be sent and received, allocate responsibility for undelivered or unintelligible communications, and stipulate the time when the contract is formed.

Electronic contracts present risks of fraud and invalid or unenforceable agreements arising from uncertainty regarding the identity, capacity and authority of the contracting parties and the authenticity of electronic communications. Various technological and practical measures may be used to reduce those risks, such as certified and secure electronic signatures, cryptography, and passwords or personal identification numbers. In some circumstances, technological measures may be supplemented with traditional

verification techniques, such as confirmation by telephone, facsimile delivery of signed and witnessed paper contracts, or credit card verification. Where identity, capacity and authority risks cannot be eliminated entirely, residual risks may be addressed through contractual risk allocation and insurance.

Document Retention and Evidence Requirements

The effective enforcement of electronic contracts requires that records of those contracts and related communications be available and admissible as evidence in legal proceedings. In addition, many laws require businesses to maintain books of account and records for a variety of other purposes. Accordingly, those engaged in electronic contracting should ensure that electronic records are retained in a manner that satisfies document retention requirements imposed by law.

Courts generally accept electronic records into evidence where there is satisfactory evidence regarding their authenticity, reliability, and trustworthiness. Many Canadian provinces have enacted electronic evidence laws to allow for the use of electronic records in evidence in legal proceedings if there is sufficient evidence of their authenticity and integrity. Accordingly, those engaged in electronic contracting should establish an electronic records management program that retains necessary electronic records and ensures the integrity of the records and the reliability and integrity of the systems in which they are maintained. In designing such a program, guidance may be found in standards published by various industry groups and government agencies.

5

INTERNET CONSUMER PROTECTION

Internet consumer protection laws provide consumers with rights and remedies regarding Internet contract formation, timely delivery, cancellation and refund, and information disclosure. A number of Canadian provinces have enacted such laws based upon a model law known as the *Internet Sales Contract Harmonization Template*, which was approved by Canadian federal, provincial and territorial governments in May 2001. The following is a brief overview of the model law.

- **Application:** The law applies to contracts formed by Internet communications regarding the supply of goods or services to consumers, provided that: (a) the supplier provides goods or services to consumers in the course of the supplier's business; (b) the consumer is an individual; and (c) the goods or services are used primarily for personal, family or household purposes. There may also be exceptions for various classes of businesses and certain types of goods or services.
- **Contract Verification:** The supplier must provide the consumer with an express opportunity to accept or decline a contract and to correct errors immediately before entering into the contract.

- **Supplier's Obligation to Provide Information:** The supplier must provide certain information to the consumer before the consumer enters into the contract, including: (a) the supplier's name and, if different, the name under which the supplier carries on business; (b) the supplier's business address and, if different, the supplier's mailing address; (c) the supplier's phone number and, if available, the supplier's e-mail address and fax number; (d) a fair and accurate description of the goods or services, including any relevant technical or system specifications; (e) an itemized list of the price of the goods or services, and any associated costs payable by the consumer, including taxes and shipping charges; (f) a description of any additional charges that may apply, such as customs duties and brokerage fees, whose amounts cannot reasonably be determined by the supplier; (g) the total amount payable under the contract and the amount of any periodic payments; (h) the currency in which amounts owing under the contract are payable; (i) the terms, conditions and method of payment; (j) the date when the goods are to be delivered or the services are to begin; (k) the supplier's delivery arrangements, including the identity of the shipper, the mode of transportation and the place of delivery; (l) the supplier's cancellation, return, exchange and refund policies, if any; and (m) any other restrictions, limitations or conditions of purchase that may apply.

  The supplier is considered to have disclosed the prescribed information to the consumer if: (a) the information is prominently displayed in a clear and comprehensible manner; and (b) the information is made accessible in a manner that ensures that the consumer has accessed the information and was able to retain and print it.

- **Supplier's Obligation to Provide Copy of Contract:** The supplier must provide the consumer with a copy of the contract in written or electronic form within 15 days after the contract is made. The contract must include all of the prescribed information referenced above, the consumer's name,

and the date the contract was made. The supplier is considered to have provided a copy of the contract to the consumer if the copy is: (a) sent by email to the address provided by the consumer for the provision of information relating to the contract; (b) sent by facsimile to the number provided by the consumer for the provision of information relating to the contract; (c) mailed or delivered to the address provided by the consumer for the provision of information relating to the contract; (d) actively transmitted to the consumer in a manner that ensures the consumer is able to retain a copy; or (e) provided to the consumer in any other manner by which the supplier can prove that the consumer received a copy.

- **Consumer's Cancellation Rights:** The consumer may cancel a contract by giving the supplier a notice that indicates the consumer's intention to cancel the contract:

  (a) at any time until 7 days after the consumer receives a copy of the contract, if the supplier does not disclose the prescribed information referenced above or the supplier does not provide the consumer with an express opportunity to accept or decline the contract or to correct errors immediately before entering into the contract;

  (b) within 30 days from the date the contract is made, if the supplier does not provide the consumer with a copy of the contract; and

  (c) at any time before delivery of the goods or the commencement of the services, if the supplier fails to deliver the goods or commence the services within 30 days after the date specified in the contract or a later date agreed to by the consumer, or if there is no date specified in the contract within 30 days after the date the contract is made.

In certain circumstances, the supplier's attempted but unsuccessful delivery of goods or provision of services will satisfy the timely delivery obligation. Also, if a court considers the consumer's cancellation of a contract to be inequitable, the court may make any order it considers appropriate.

- **Effect of Cancellation:** The consumer's lawful cancellation of a contract operates to cancel the contract as if it never existed, and also cancels any related consumer transaction, any guarantee given in respect of the contract, any security given by the consumer or a guarantor in respect of the contract, and any related contract for credit extended or arranged by the supplier.
- **Cancellation Responsibilities:** If a contract is cancelled by the consumer, the supplier must, within 15 days, refund to the consumer all consideration paid by the consumer under the contract and any related consumer transaction. If goods are delivered to the consumer under a cancelled contract, the consumer must, within 15 days after the later of the date of cancellation or delivery of goods, return the goods to the supplier unused and in the same condition in which they were delivered. The supplier must accept the goods and pay for the cost of their return.
- **Credit Card Refunds:** A consumer that has charged to a credit card account all or any part of the consideration payable under a contract may request the credit card issuer to cancel or reverse the credit card charge and any associated interest or other charges if the supplier fails to refund all of the consideration within 15 days after the consumer cancels the contract. The consumer's request must be in writing or electronic form, provide details of the contract, state the reason for the cancellation, indicate the date and method of cancellation, and provide other prescribed information. If the consumer's request meets the requirements, the credit card issuer must cancel or reverse the credit card charge and any associated interest or other charges within the earlier of two complete billing cycles or 90 days.
- **Other Consequences of Non-Compliance:** In addition to the remedies and consequences outlined above, a contravention of, or failure to satisfy, certain requirements by the supplier or credit card issuer is an offence punishable by fines, imprisonment, and other court ordered corrective measures.

The various provincial laws will likely also provide that the Internet consumer rights and remedies cannot be avoided, limited or modified by agreement, and are in addition to any other rights or remedies the consumer may have by agreement or at law, including other consumer protection and sale of goods laws.

To comply with Canadian Internet consumer protection laws, Internet business-to-consumer suppliers should use a multi-step ordering process in which consumers click through: (a) an order verification screen that provides them with an opportunity to correct errors they may have made in the ordering process; and (b) a screen that presents all prescribed information regarding the proposed transaction and an opportunity to download and print the information before the transaction is completed.

6

INTERNET ADVERTISING

Advertising on the Internet is subject to the same laws as advertising in print and other media. In Canada, advertising is regulated by provisions of the *Criminal Code*, the *Competition Act*, and provincial consumer protection and business practices statutes. Generally, those laws prohibit advertising and other marketing practices that are false, misleading, unfair or deceptive, and require claims regarding the performance, efficacy or durability of a product to be substantiated by adequate and proper testing. Those laws also impose specific requirements regarding certain marketing practices, such as contests and multi-level marketing plans, and prohibit other practices.

The nature of Web sites and other Internet communications, including the use of links, multimedia content, and other technologies, presents risks of inadvertently violating advertising laws. The inability of Internet consumers to physically inspect products available for sale over the Internet increases their reliance on Internet advertising, and the advertiser's potential liability for advertising that is misleading.

Government agencies have issued guides to assist Internet advertisers in complying with advertising laws. For example, the Canadian Competition Bureau published *Staying 'On-side' When Advertising On-line: A Guide to Compliance with the Competition Act When Advertising on the Internet* (available online: *www.strategis.ic.gc.ca/SSG/ct02186e.html*), and the U.S. Federal Trade

Commission published *Advertising and Marketing on the Internet: Rules of the Road* and *Dot Com Disclosures* (available online: *www.ftc.gov/bcp/menu-internet.htm*).

The following is a summary of some important considerations regarding Internet advertising:

- Advertising laws apply not only to Web sites, but to all forms of on-line advertising and marketing, including e-mail and chat room postings, made for the purpose of promoting the supply or use of a product or a business interest (whether purchased on-line or off-line) or influencing other consumer conduct.
- Advertising must be truthful, fair and not misleading. Claims regarding products must be substantiated. Illustrations, photographs, artwork and audio-visual representations regarding a product or service should be accurate.
- Generally, any representation that is false or misleading in a material respect is prohibited. A representation is material if it could influence a consumer's course of conduct. To determine whether a representation is false or misleading, courts consider the general impression it conveys, as well as its literal meaning.
- Internet advertisements should be assessed from the perspective of the average consumer who is interested in the product or service being promoted. Also, special care should be taken regarding advertising targeted to children or other classes of consumers who may not have the capacity to understand fully the information presented to them.
- Disclaimers, qualifications, and other information required to be disclosed to ensure that a representation does not create a false or misleading impression should be clear and conspicuous, located in proximity to the representation to which they relate, and presented so that they will be seen.

- The effectiveness of a disclaimer will be determined by the general impression conveyed by the advertisement as a whole. The following should be considered in determining whether an on-line disclaimer is sufficient: (a) the location of the disclaimer on the Web site relative to the principal representation; (b) the layout of the Web page and the likelihood that the disclaimer will be read; (c) the use of attention-grabbing tools that provide notice of the disclaimer; (d) the size and colour of font used in the disclaimer; and (e) the accessibility of the disclaimer by all potential users.
- Hyperlinks are often used to provide additional information regarding general advertising statements, including disclaimers, disclosures, and related rules, terms or conditions. The following are some suggestions regarding the use of hyperlinks: (a) links should be placed near the information to which they relate; (b) links should be obvious; (c) links should be labelled to indicate the importance, nature and relevance of the linked information; (d) link styles should be consistent, so that users know when a link is available; (e) the effectiveness of links should be assessed (by monitoring click-though rates) and necessary changes should be made.
- To avoid making misleading representations, advertisers engaged in electronic commerce should provide accurate information about transaction terms, conditions and costs, including the following: (a) the full price and other costs and charges; (b) delivery terms, including timing, cost and method; (c) payment terms, conditions and methods; (d) geographic or time limitations; (e) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund, and any related time limitations or associated fees; (f) product warranties, guarantees, limitations and conditions; (g) services standards, schedules, and fees; and (h) other terms, limitations and conditions. Internet

consumer protection laws impose detailed consumer transaction disclosure requirements.

- Advertisers must ensure that they live up to the representations they make regarding their policies and practices. In particular, representations regarding privacy policies should be truthful and not misleading. Failure to comply with stated policies and practices may result in liability for misleading advertising and fraudulent and deceptive trade practices.
- Contests must not violate criminal law prohibitions against gaming and lotteries, and must include fair and adequate disclosure, including information regarding contest rules and facts that materially affect the chances of winning.
- Liability for misleading advertising may be imposed not only on the person who caused the advertisement to be made, but also on others involved in the advertisement, such as advertising agencies and traditional media providers and their electronic commerce counterparts – Web page designers, proprietors of cyber-malls and electronic bulletin boards, chat room operators and Internet service providers. Criminal liability generally requires that the impugned misrepresentation be made "knowingly or recklessly". Civil liability may not require such an intention. The *Competition Act* provides a "publisher's exemption" for a person who prints or publishes or otherwise disseminates an advertisement on behalf of another person in Canada, provided that the publisher accepts the advertisement in good faith for printing, publishing or dissemination in the ordinary course of business and obtains and records the name and address of the person who places the advertisement.
- The global nature of the Internet means that on-line advertisements made by a person located in Canada may be viewed by consumers all over the world, thereby resulting in potential liability not only under Canadian law but under foreign laws as well. Canadians making on-line

advertisements should ensure that they comply with applicable Canadian laws, and may wish to seek legal advice regarding compliance with foreign laws. Persons outside Canada making on-line advertisements may be subject to Canadian laws if the advertisements are available to, and might reasonably be expected to materially influence, Canadians. To reduce the risk that advertisements are considered to be directed at foreigners, on-line advertisers should: (a) clearly indicate the persons for whom the advertisements are intended or, alternatively, the persons for whom the advertisements are not intended; (b) require users to indicate their country of residence, and then link them to the appropriate Web site; (c) use screening technologies to restrict Web site access to consumers from countries to which advertisements are directed; and (d) only enter into contracts with consumers from countries to which the advertisements are directed as confirmed by information such as delivery or payment addresses.

Government agencies are expected to continue to assess the application of advertising laws to the internet, and to issue further guidance from time to time. Laws specifically directed to Internet advertising may also be enacted. Internet advertisers should monitor those and other legal developments and regularly review their advertising practices to ensure compliance with applicable laws.

7

WEB SITE DEVELOPMENT

Developing a Web site presents numerous business and legal issues. To avoid difficulties or disputes, Web site owners and developers should enter into written agreements that set forth their respective obligations, rights, and remedies, and allocate business and legal risks.

There are usually a number of phases in a Web site development project: *discovery* (an assessment of the organization and its marketing approach, and the intended purposes and desired functionality of the Web site); *design and planning* (the creation of detailed specifications regarding the look, feel and functionality of the Web site and the project plan); *development* (the computer code implementation of the specifications in accordance with the project plan); *acceptance testing* (the testing of the Web site and the correction of bugs or deficiencies); *deployment* (putting the Web site into production on an Internet-connected computer); and *support and maintenance* (the ongoing maintenance and development of the Web site).

Like any other complex project, it is important to plan a Web site development project carefully, and to address important business and legal issues before problems arise. The following are some suggestions regarding issues commonly addressed in a Web site development agreement.

- **Discovery:** The agreement should describe the developer's discovery obligations, the required involvement of the owner and its personnel, and the report to be delivered by the developer at the conclusion of the

discovery phase. The agreement should also set forth the owner's right to terminate the agreement after the conclusion of the discovery phase.

- **Design:** The design phase should result in clear specifications for the Web site and the development project. Specifications usually include the following: (a) Web site design, content, and functionality (including required server hardware and third party software, Internet-browser compatibility, and performance metrics); (b) development timeline; (c) interim deliverables; and (d) final deliverables. The agreement should describe the developer's obligations to deliver detailed draft specifications regarding the Web site, the owner's obligation to review and provide comments regarding the draft specifications, and the developer's obligation to deliver revised specifications that remedy deficiencies identified by the owner. The agreement should also set forth the owner's right to terminate the agreement after the conclusion of the design phase.

- **Project Team:** Owners often select developers based upon their experience and the proposed project team. Accordingly, the agreement should identify the developer's project manager and other personnel, require that they be available to work on the project as needed to ensure timely performance, provide for owner approval regarding personnel changes, and provide the owner with termination and other remedies if the required project team is not available. The agreement should also indicate whether or not the developer is allowed to hire subcontractors to work on the project.

- **Timing, Cost & Payments:** The agreement and specifications should provide a clear timetable for each phase of the project and stipulate the amounts payable upon the completion of each milestone. The agreement should stipulate the total cost of the project. Web site project costs may be fixed or based upon time and materials. Hourly rates for each project team member should be indicated, and the maximum cost of each phase of the project should be stipulated. A reasonable payment schedule (with

payments weighted toward final delivery) will create an incentive for the developer to complete the project in a satisfactory and timely manner.

- **Content Responsibilities and Control:** The agreement should allocate, as between the owner and the developer, responsibility for providing Web site content. The agreement should provide that if the developer obtains content from third parties, the developer must also obtain licences and waivers for the owner to use the content for the Web site. The owner should have absolute control over Web site content.
- **Deliverables:** The agreement should indicate all of the interim and final deliverables the developer must provide to the owner, including Web site content in paper and electronic format, underlying Web site software and implementation coding in both object code and source code, logic manuals and flow charts, licenses for third party content and software, and all other materials necessary for the owner's operation, support, maintenance and modification of the Web site.
- **Acceptance Testing:** The agreement should set forth the procedure to be followed regarding the owner's testing and acceptance of the Web site and related deliverables, and the developer's obligation to correct bugs and deficiencies.
- **Correction of Defects:** The agreement should describe the developer's obligation to correct any Web site defects discovered during a specified period of time after acceptance.
- **Deployment:** The agreement should describe the developer's obligations regarding the deployment of the Web site on the host server.
- **Support and Maintenance:** The agreement should describe the developer's obligations regarding the future support and maintenance of the Web site.

- **Additional Services:** The agreement should describe any additional services required of the developer and the costs of those services. Common additional services include training, periodic upgrades and additions to Web site content, further Web site development, and Web site promotion through registration with Internet search engines and directories.
- **Ownership:** The agreement should allocate ownership and use rights in the Web site and its components, including appropriate copyright assignments and licences and moral rights waivers. In the absence of those provisions, the Web site owner might not have the rights necessary to use the Web site and its components in the intended manner. The agreement should also provide for the ownership of work in progress in the event the agreement is terminated before the project is completed.
- **Warranties, Representations and Indemnities:** The agreement should include various developer representations and warranties, including that the owner's use of the Web site and its components will not infringe other persons' rights. The developer should also agree to indemnify the owner against claims by other persons for violations of their rights resulting from the development or the use of the Web site (excluding claims relating to Web site content provided by the owner).
- **Liability Disclaimers, Exclusions, and Limitations:** The developer may require that the agreement include liability disclaimers, exclusions and limitations that restrict the developer's responsibility to compensate the owner for damage and loss resulting from the developer's breach of the agreement. The owner should assess the business and legal risks presented by those provisions and consider alternative measures to reduce those risks, such as appropriate termination rights, self-help remedies and adequate insurance.

- **Termination:** The agreement should stipulate the developer's and owner's respective termination rights and remedies and the consequences of termination, including termination for cause or convenience, the form and length of termination notice, and the fees or pre-estimated damages payable by the defaulting or terminating party.
- **Development Credit:** The agreement should indicate the manner, if any, in which the developer may use the Web site as a marketing tool, and whether the Web site will indicate the developer's involvement in the site (known as a "development credit clause").
- **Exclusivity:** The agreement should describe any restrictions on the developer's ability to create a Web site for the owner's competitors.
- **Confidentiality:** The agreement should require the developer and its employees and subcontractors to keep confidential all information they obtain regarding the Web site and the owner's business and customers. The agreement should require the developer to return to the owner at the conclusion of the project all paper and electronic documents and data obtained from the owner during the project.
- **Insurance:** The agreement should indicate whether the owner or developer are required to obtain insurance coverage for potential risks and liabilities arising from the project or the owner's use of the Web site.

8

WEB SITE HOSTING

Many Web site owners lack the technical competence or resources necessary to host their own Web sites. Instead, they contract for Web site hosting and related services. The satisfactory operation of a Web site will depend upon the services, resources, and reliability of the Web site host. For this reason, Web site owners and hosts should record their agreement in a Web Site Hosting Agreement. Failure to do so may result in costly disputes.

A Web Site Hosting Agreement should stipulate the parties' respective obligations, rights and remedies, and fairly allocate the risks inherent in hosting a Web site. The following are some suggestions regarding issues commonly addressed in a Web Site Hosting Agreement.

- **Hosting Services Specifications and Performance Criteria:** The agreement should stipulate the required Web site hosting services, including: (a) server hardware and software configuration, storage space, and redundancies, including whether the server and server-Internet connection will be dedicated or shared; (b) Web site performance criteria, including availability (uptime), bandwidth, response time and transmission speed, the maximum number of simultaneous users, scheduled downtime, and scalability; (c) technological and physical security measures and disaster-recovery measures, including back-up server capacity; (d) data back-ups; (e) monitoring, maintenance and problem response time during normal business hours and after hours; (f) secure

owner access for updating the Web site, downloading data, and monitoring Web site performance; (g) timely implementation of changes to the Web site; and (h) routine delivery of a complete electronic copy of the Web site and related data to the owner. The agreement may also require the host to acquire and use up-to-date technologies when they become commercially available.

- **Other Services:** The agreement should stipulate all other services to be provided by the host, including technical assistance and support, software and other tools necessary for the owner to access and modify the Web site, email, file transfer protocol (FTP), and regular reports regarding site transactions and user information. If the Web site is to be used for commercial transactions, secure transaction support is essential and the encryption and other required services should be stipulated in the agreement.
- **Fees:** The agreement should stipulate the costs for hosting and all other services, including appropriate mechanisms for fee adjustments if usage volumes and service demands exceed expectations, and fee credits if hosting services are below contractual standards.
- **Remedies:** The agreement should stipulate the Web site owner's rights and remedies, and the host's corresponding obligations, if there is a Web site failure, security breach, or other malfunction, or if the host fails to meet stipulated performance criteria. The owner's remedies may include termination rights and pre-estimated damages.
- **Web Site Content:** The agreement should prohibit unlawful, abusive or offensive Web site content or use (such as sending bulk unsolicited email), and permit the host to deactivate the Web site if those prohibitions are breached. The agreement should also provide a procedure for responding to third party complaints and disputes regarding the Web site. The agreement may also require the owner to indemnify the host against claims relating to the Web site.

- **Warranties, Representations and Indemnities:** The agreement may include various representations and warranties by the owner and the host, including non-infringement of other person's rights, and agreements to indemnify each other against claims by other persons for violation of their rights.
- **Liability Disclaimers, Exclusions, and Limitations:** The agreement may include liability disclaimers, exclusions and limitations. The owner and host should assess the business and legal risks presented by those provisions and consider alternative measures to reduce those risks, such as appropriate termination rights, self-help remedies and adequate insurance.
- **Confidentiality and Customer Information Privacy:** The agreement should require the Web site host and its employees to respect the confidentiality and privacy of information regarding the owner's business and customers, transactions occurring through the Web site, and Web site users' personal information. The agreement should also require the host and its employees to comply with all applicable privacy laws and industry codes. The agreement may also describe the host's data retention and destruction obligations.
- **Ownership and Control:** The agreement should confirm that the Web site owner has exclusive ownership of the Web site and its content, and exclusive control over the Web site content and any changes to the content. The agreement should also acknowledge the Web site owner's exclusive ownership of the Web site domain name.
- **Commercial Exploitation:** The agreement may impose restrictions regarding the host's ability to publicly disclose that it is the host of the Web site.

- **Termination and Transfer:** The agreement should stipulate the parties' respective termination rights and remedies and the consequences of termination, including the ability to terminate for cause or convenience, the form and length of termination notice, and the fees or pre-estimated damages payable by a defaulting or terminating party. The agreement should require the host to reasonably cooperate and assist in the transfer of the Web site to a new host; to return data, documents, and information regarding the Web site and its operation to the owner; to continue the operation of the Web site for a reasonable time to allow for its transfer; and to maintain a link to the new Web site location and forward email for a reasonable time after the Web site is transferred.
- **Insurance:** The agreement should indicate whether the owner or host are required to obtain insurance coverage for potential risks and liabilities arising from the Web site.

9

WEB SITE USE AGREEMENTS

A Web site use agreement (often called "terms of use") protects the Web site owner's business and legal interests and limits its potential liability. Appropriate Web site use agreement terms depend upon the nature of the Web site and the business and legal risks it presents.

Typical Provisions

The following are some provisions typically found in a Web site use agreement:

- **Acceptance and Amendment:** Web site use agreements should clearly indicate that they are binding agreements between the user and the Web site owner. They should also indicate the manner in which they may be amended by the Web site owner.
- **Permitted Users and Access:** Web site use agreements often prohibit use by minors, because they cannot create valid and binding contracts and because there may be legal restrictions regarding the collection and use of information about minors. Web site use agreements also often restrict Web site use to persons located in specified jurisdictions to reduce the risk of the Web site owner being held to be carrying on business in other jurisdictions and subject to their laws and the jurisdiction of their courts.

- **Termination of the Agreement and Access:** Web site use agreements should provide the Web site owner with a contractual, discretionary right to change or terminate the Web site and to temporarily or permanently deny access to particular users. Web site use agreements should identify the provisions that survive the termination of the agreement.
- **Fees and Charges:** Web site use agreements should describe all fees and charges associated with the use of the Web site.
- **General Disclaimer of Liability, Indemnity, Release:** The operation of a Web site may be affected by factors beyond the owner's control. Accordingly, Web site use agreements should disclaim any responsibility or liability for such matters. Web site use agreements may require users to indemnify the Web site owner for any liabilities or expenses resulting from the user's breach of the Web site use agreement or other wrongful acts.
- **Privacy:** It is increasingly common for Web site use agreements to incorporate by reference a Web site privacy policy.
- **User Names and Passwords:** Web site use agreements may impose certain restrictions, obligations and liabilities regarding the use and disclosure of user names and passwords.
- **Web Site Ownership, Use and Restrictions:** Web site use agreements should: (a) include statements regarding the ownership of the Web site and its content; (b) define the rights afforded to users regarding the Web site content; and (c) set forth restrictions regarding the use of the Web site and its content. For example, Web site use agreements typically prohibit unauthorized linking, framing and data-mining.
- **Trade-mark Information:** Web site use agreements should include notices regarding the trade-marks used on the site, and should prohibit the unauthorized use of the marks.

- **Links to Other Sites:** Web sites often contain links to other Web sites. To reduce the risk of liability for those other sites, Web site use agreements may warn users that links to other Web sites are provided for convenience only, and should disclaim any responsibility or liability for those other Web sites.
- **Postings and Submissions:** Users often send ideas or suggestions to Web sites or Web site owners. To limit the risk of liability for unauthorized use of those ideas or suggestions, Web site use agreements may provide that any submission of ideas or suggestions constitutes the grant of a licence to use the ideas and suggestions and anything derived from them without any confidentiality or compensation obligations.
- **Software Licence Agreements:** If software is available for downloading through the Web site, the Web site use agreement may provide that the software is protected by copyright and that the downloading and use of the software is subject to a specific software licence agreement.
- **Contests:** Web site use agreements may warn users that their participation in contests available through the Web site is subject to specific contest rules. Appropriate contest rules and procedures are necessary to comply with advertising laws and avoid violating criminal gaming laws.
- **Governing Law and Dispute Resolution:** Web site use agreements should stipulate the law that governs the relationship between the Web site owner and the user, the forum (arbitration or court) and location for the resolution of any disputes, and any contractual time limits for the commencement of legal proceedings.
- **Information Postings and Discussion Groups:** If users post information or participate in discussion groups through the Web site, the Web site use agreement should require compliance with rules governing postings and discussions (including rules regarding monitoring and complaints,

compliance, consequences, and law enforcement disclosure), and should provide for a complaint process.

- **Transaction Issues:** If the Web site facilitates electronic transactions, the Web site use agreement should address electronic contracting issues (offer and acceptance, product availability, misprints and errors, and order processing) and should include standard product-related and service-related disclaimers, liability exclusions, and limitations. If the Web site uses specific agreements for each transaction, the Web site use agreement should warn users that each transaction is governed by a specific transaction agreement.
- **Other Matters:** Web site use agreements may also contain provisions relating to other matters typically found in a commercial or consumer contract, including severability of invalid or unenforceable provisions, waiver, integration, conflicts with other agreements, and assignment.

Effective Implementation

To be effective, a Web site use agreement must be a valid and enforceable contract between the Web site owner and Web site users. In Canada, the formation of valid electronic contracts is governed by laws regarding electronic commerce and Internet consumer protection.

There are several ways in which a Web site use agreement may be implemented, including as a "click-through" agreement or a "notice-and-acceptance-by-conduct" agreement, both of which are discussed in the previous chapter regarding electronic contracts. In addition to the initial implementation of the Web site use agreement, users should be reminded of the agreement each time they log into the Web site and in Web site-related email and other communications. Also, printed versions of the agreement may be sent to users with goods purchased through the Web site.

It is important to maintain reliable electronic and paper records regarding the implementation of a Web site use agreement, including the different

versions of the agreement as amended from time to time. It is also important to maintain reliable records of Web site use, communications and transactions. Those records may be required for regulatory purposes and to respond to investigations, complaints, or claims. Accordingly, it is important to implement security and back-up procedures that will ensure that all such records are reliable and that their integrity has not been compromised.

10

PERSONAL INFORMATION PRIVACY

Many Web sites collect personal information voluntarily provided by users, such as their names, email addresses, postal addresses, and credit card information. Some Web sites also automatically collect non-identifiable information about users and the manner in which the Web site is used. The collection, use and disclosure of personal information present significant privacy and confidentiality issues.

Privacy Laws

The Canadian *Personal Information Protection and Electronic Documents Act* and similar laws of other jurisdictions, including the United States *Children's Online Privacy Protection Act of 1998*, have recently been enacted to govern the collection, use and disclosure of personal information. The European Union has enacted a *Directive* governing the processing of personal information and imposing stringent restrictions on the movement of that information to and from EU member countries.

There are also numerous non-binding codes and guidelines that address those issues, such as the Canadian Marketing Association's *Code of Ethics and Standards of Practice*.

Web Site Privacy Policies

Privacy laws and regulatory codes generally require that Web site owners obtain Web site users' informed consent to the collection, use and disclosure of their personal information, and give Web site users reasonable access to their collected personal information and an opportunity to correct erroneous information. Generally, consent is obtained by publishing a detailed privacy policy. The following are some issues typically addressed in Web site privacy policies:

- **Consent:** The privacy policy should provide that use of the Web site signifies that users consent to the Web site owner's collection, use and disclosure of their personal information in accordance with the policy.
- **Non-Identifiable Information**: The privacy policy should permit the Web site owner to gather non-identifiable information about Web site users, such as the Internet Protocol address of their computers and Internet service providers, the dates and times they access the Web site, the Web sites from which they linked to the Web site, and their activities on the Web site. This data can provide a great deal of information about the manner in which the Web site is being used, and how it can be improved.
- **Tracking Information**: The privacy policy should allow the Web site owner to use non-identifiable information to create aggregate tracking information regarding user demographics, traffic patterns and, where appropriate, to provide those aggregated reports to advertisers or others. If tracking information is linked to Web site users' personal information, it should be treated as personal information.
- **Cookies**: Many Web sites use "cookies", a technology that installs a small amount of information on a Web site user's computer so the Web site can recognize future visits using that computer. Cookies may be used to track an individual user's activity on the Web site and to offer more personalized Web page content and information. The privacy policy should disclose whether and how cookies are used.

- **Personal Information Specifically Provided**: The privacy policy should indicate the kinds of personal information that users may be required to voluntarily submit when using the Web site and explain how the Web site owner may use that information.
- **Unsolicited Email**: The privacy policy should indicate whether the Web site owner will send unsolicited email to users, and explain how users may choose to opt in or opt out of receiving unsolicited email.
- **Disclosure of Personal Information**: The privacy policy should indicate whether the Web site owner intends to disclose users' personal information to affiliates, trading partners, or service-providers, in the course of business transfers, or for law enforcement or legal proceedings. If personal information is to be disclosed, an appropriate *Data Privacy Agreement* should be entered into with the data recipients to require that they protect the privacy of the information. The privacy policy should indicate the names of the data recipients and explain whether users may elect not to have their personal information disclosed.
- **Location of Information**: The privacy policy may inform users where their personal information will be stored and processed.
- **Security**: The privacy policy should warn users that security and privacy risks cannot be eliminated, and explain the safeguards the Web site owner uses to protect the confidentiality of the information.
- **Accessing Personal Information**: The privacy policy should enable users to obtain reasonable access to their collected personal information and challenge its accuracy or completeness. Where users' personal information is inaccurate, it should be amended.

- **Other Agreements**: The privacy policy may also remind users that their use of the Web site is governed by other agreements, such as a Web site use agreement.
- **Former Users**: The privacy policy may explain how the Web site owner will use the personal information of former users.
- **Policy Changes**: Information practices and Internet technologies change rapidly. The privacy policy should provide that it may be changed from time to time, and explain how users will be notified of policy amendments. It should also explain how policy amendments will apply to previously gathered personal information.

Implementing a Web Site Privacy Policy

Effective implementation of a Web site privacy policy is essential. Failure to comply with a policy may give rise to liability for consumer fraud, breach of applicable personal information privacy laws, and breach of contract. The following are some suggestions regarding the implementation of a Web site privacy policy.

- **Dissemination**: Inform all employees of the policy and require that they comply with its provisions and otherwise respect personal information privacy.
- **Privacy Managers**: Designate individuals as privacy managers who are accountable for compliance with the policy and are trained to respond to complaints and inquiries.
- **Changes to the Policy**: Inform users by email if the privacy policy will be changed.
- **Records**: Maintain records of all use and disclosure of personal information.
- **Email**: Ensure that all unsolicited email sent to Web site users informs them how to decline further email.

- **Security**: Implement adequate security measures to protect the confidentiality of personal data.
- **Information Retention and Destruction**: Establish and implement an appropriate personal information retention and destruction policy.

11

COMMUNICATIONS SYSTEM RISK MANAGEMENT

Modern communications systems present significant business and legal risks. Communications system misuse can reduce productivity and profitability, impose significant additional costs, and result in costly litigation and substantial legal liabilities.

Every organization should address those concerns by adopting and implementing a written communications system policy ("CSP") governing the use of the Internet, intranets and extranets, email and voice mail ("vmail"). A CSP should educate employees, contractors and other systems users regarding communications system risks and liabilities, and should prescribe the ways in which the system may be used.

Communications System Risks

- **Internet Risks:** Internet data transmission can result in the deliberate or inadvertent violation of copyright and other intellectual property rights, breach of confidentiality obligations, trade secret misappropriation or disclosure, and violation of local and foreign criminal laws. Internet transmission of unencrypted data is not secure – the data is vulnerable to unauthorized access as it travels across the Internet. Many Internet users falsely believe they are anonymous in cyberspace. This misconception may lead them to engage in inappropriate or illegal conduct. Internet

access can be a distraction that reduces user productivity, consumes system resources and degrades system performance.

- **Intranet and Extranet Risks:** Intranets (internal, private networks) are typically used to disseminate information within an organization. Extranets (restricted access, private networks) allow authorized users to access an organization's internal information. Intranets and extranets generally present the same risks as the Internet, and may also present additional security, privacy and confidentiality risks.

- **Email Risks:** Email has distinct qualities that account for its popularity and utility, but which also contribute to its risks. Consider the following: (a) email is typically casual, conversational and spontaneous, tends to be created with less care than more formal communications, and often contains ill-considered and potentially damaging statements; (b) email can be effortlessly reproduced, distributed and redistributed to innumerable recipients inside and outside an organization at virtually no cost; (c) a click of the wrong button can result in immediate and irretrievable distribution of email to numerous unintended recipients; (d) email can be forwarded to unintended recipients; (e) it is relatively easy to forge email (known as "spoofing") or to alter someone else's email before forwarding it to others; (f) email can be lost or delayed due to causes beyond the control of the sender or recipient; (g) email provides more detailed information than ordinary paper communications (i.e. who created the email, when and to whom it was sent, and in some cases when it was received and read); (h) email is almost always recoverable and is usually more difficult to eliminate than are paper communications; and (i) email is susceptible to unauthorized access at each computer where an electronic copy of the email resides, and each filing cabinet where paper copies of the email are stored. For these reasons, email can be an electronic "smoking gun" in legal proceedings.

- **Vmail Risks:** Vmail presents many of the same benefits and risks as email. Vmail messages can be saved, recorded or transcribed, and used as evidence.

Communications System Liabilities and Other Concerns

- **Liabilities:** Businesses may bear direct or vicarious civil liability for the misuse of their communications systems. In certain circumstances, businesses can bear criminal liability for such misconduct. Communications system misconduct can also result in embarrassing negative publicity for the user and the organization. One factor that contributes to the risk of organization liability and embarrassment is the use of email addresses that contain the organization's name, i.e., *employee@organization.com*.
- **Litigation Disclosure:** Email, computer calendars and diaries, and other electronic records are generally discoverable and admissible into evidence in legal proceedings. For the reasons discussed above, electronic evidence disclosed in litigation and revealed in open court can be embarrassing and harmful. In addition, producing electronic records in response to litigation disclosure obligations can be a considerable logistical burden and impose a significant cost, particularly if the electronic records are not properly indexed and stored.
- **Privacy:** Businesses have a legitimate interest in monitoring communications system use, accessing user email and other data, and disclosing electronic information for business reasons or to fulfill legal obligations. Nevertheless, unauthorized access to, or use or disclosure of, private communications, including email and computer files, may violate privacy rights, breach employment agreements, constitute an unfair labour practice, or give rise to civil or criminal liability. In addition, information obtained through an unreasonable invasion of privacy rights might be excluded from evidence in legal proceedings. Those risks may be addressed by obtaining users' express consent to the monitoring, use and disclosure of their communications system use and data.

- **Security:** Communications systems present a number of internal and external security concerns, including unauthorized access from both inside and outside the system, viruses and the physical security of system hardware and data.
- **Confidentiality and Privilege:** Confidential information and trade secrets can lose their protection through inappropriate and unrestricted disclosure. Similarly, solicitor-client privilege (a client's legal right to refuse to disclose legal advice) can be lost if a privileged communication is disclosed to others.
- **User Productivity and System Performance:** Certain communications system components, and particularly Internet access, can distract users and reduce productivity. Also, communications system abuse and misuse can drain system resources, degrade system performance and compromise system integrity.

Risk Management – Creating a Communications System Policy

A clear and comprehensive CSP can enhance communications system benefits and reduce communications system risks. A CSP should be prepared with proper legal advice to ensure that it is consistent with applicable laws and contractual obligations, including collective bargaining agreements. It should also be prepared with proper technical advice. Proper implementation of a CSP is critical, and a senior management person should be made responsible for the CSP implementation.

The following are some of the issues that should be considered in preparing a CSP:

- **User Education:** One of the most important functions of a CSP is to educate users about the potential risks and liabilities associated with communications technologies. There should be ongoing training, periodic updates and reminders.

- **System Use:** A CSP should prescribe system use rules. The rules may range from restrictive (business-only use) to liberal (unrestricted use subject to stipulated prohibitions and non-interference with productivity). A CSP that permits business-only uses may reduce certain risks, but it may be difficult to enforce. At the very least, a CSP should require system use to be lawful and consistent with the organization's general reputation, standards and other work-place conduct rules and productivity expectations. A CSP might also prohibit specific uses and participation in certain Internet activities, such as Internet chat rooms and discussion groups.

  It may be also appropriate to stipulate email use, content and etiquette protocols. For example, requiring receipt confirmation for important email, restricting the use of "All Users" email, or requiring authentication of business-related email and the use of disclaimers on non-business email. A CSP should establish procedures that protect the organization's legitimate interests, but are not so rigid as to reduce or possibly eliminate email's productivity benefits.

- **Monitoring, Use and Disclosure:** A CSP should advise all users that there is no privacy regarding communications system uses and data, including email and vmail, and that the organization reserves the right to monitor, use and disclose communications system uses and data without further notice, but has no obligation to engage in such monitoring. The CSP should establish proper procedures for the monitoring, use and disclosure of communications system use and data. Decisions regarding monitoring system use and reviewing and disclosing data ought to be made by senior personnel with the benefit of proper legal advice.

- **Security:** Communications systems are vulnerable to internal and external security threats. Organizations may implement technological security measures, and may also take common sense security precautions, such

as requiring the use of password-protected screen savers and distributing system access usernames and passwords in a secure manner. Information technology ("IT") personnel may have access to user passwords and other security-related information that may be misused with serious consequences. Accordingly, there should be careful pre-hiring screening of all IT personnel, and routine post-employment procedures should be established and followed.

- **Confidentiality Protocols:** External email is not secure or private unless it is encrypted. Accordingly, a CSP may prohibit the use of unencrypted external email for sending or receiving confidential information, including trade secrets and privileged information, and require all external email to be marked with a confidentiality warning. A CSP may also require that internal email containing confidential or privileged information be properly labelled as "Confidential" or "Privileged".
- **Encryption Protocols:** The uncontrolled use of data encryption can interfere with data access and system monitoring and maintenance. Accordingly, a CSP may contain encryption guidelines regarding permissible encryption methods and when encryption should and should not be used.
- **Data Retention and Destruction:** A CSP should include a data retention policy to ensure that electronic data is organized, archived and stored in a secure manner that provides for efficient retrieval. It should also attempt to minimize the accumulation of unnecessary data.
- **Software Management:** For legal and practical reasons, a CSP may prohibit the use of software that is not properly licensed and approved by IT personnel.
- **Compliance:** Users ought to be warned that CSP violations may result in discipline corresponding to the gravity of the offence, including termination of system access or summary dismissal.

- **Implementation:** It is important to ensure that all system users, including permanent and temporary employees, contractors, and consultants, are given notice of the CSP and agree to abide by it. This may be done in various ways. The safest course is to require all users to sign a written acknowledgement that they have read, understood and agreed to the CSP. Alternatively, usernames and passwords may be distributed with a copy of the CSP and a notice that use of the communications system constitutes acceptance of the CSP and agreement to its terms. Another alternative is to have the system log-on process require users to accept the CSP by clicking an "I ACCEPT" button. The CSP should state that use of the system constitutes acceptance of the CSP and agreement to its terms. The CSP should also be included in all relevant policy manuals. Also, users should be reminded of the CSP on a regular basis. For example, reminders may be displayed during the system log-on process, and may be communicated periodically by memorandum or email.
- **Insurance:** As part of a CSP preparation process, it is prudent to ensure that adequate insurance is in place to cover potential communications system liabilities.

Communications systems will continue to evolve. CSPs and their implementation should be reviewed on a periodic basis and revised as necessary. The review process may also provide valuable information that can be used to improve the system and to identify and address new risks and liabilities.

12

SECURITIES REGULATION AND THE INTERNET

The Internet is a valuable tool for securities issuers, financial service providers, and investors. Nevertheless, the Internet presents considerable challenges for securities market participants seeking to ensure that their Internet activities comply with applicable laws, and for regulators seeking to protect investors and the integrity of capital markets. Regulators have issued various policies and guides regarding the application of securities laws to Internet activities. The following is a brief overview.

- **Securities Laws Apply:** Securities regulators in Canada and elsewhere have rejected the proposition that cyberspace is a separate jurisdiction in which securities activities are immune from traditional laws, and have asserted that general securities laws apply to Internet activities. Web sites, email and other electronic communications will be considered to be additional media for the distribution of information, and their use will generally be required to comply with securities laws in the same manner as communications using print and other traditional media.
- **General Regulatory Jurisdiction:** Securities regulators have taken the position that they may regulate Internet conduct that originates from within their territorial jurisdiction, and also conduct originating outside their territorial jurisdiction that is directed to persons within their jurisdiction or that has adverse effects within their jurisdiction.

- **Jurisdiction Over Targeted Internet Communications:** Targeted communications methods, such as directed email and mass emailing, are comparable to traditional mail because the sender directs the information to a particular person, group or entity. Persons using such targeted technologies must identify when communications are being sent to persons in foreign jurisdictions and ensure that those communications comply with foreign securities laws.

- **Jurisdiction Over Web Sites:** Web site postings are different from targeted communications because they are not sent to any particular person and are available for anyone with Internet access. Canadian securities regulators have indicated that they will generally consider a person to be trading in securities in a local jurisdiction if the person posts on the Internet a document that offers or solicits trades of securities and is accessible to persons in that local jurisdiction, unless: (a) the document contains a prominently displayed disclaimer that expressly identifies the jurisdictions in which the offering or solicitation is qualified to be made, and that identification does not include the local jurisdiction; and (b) reasonable precautions are taken not to sell to anyone resident in the local jurisdiction. A similar approach has been taken by the United States Securities and Exchange Commission and other foreign securities regulators.

- **Electronic Delivery of Documents:** Securities law obligations to deliver documents (such as prospectuses, financial statements, trade confirmations, account statements, and proxy-related materials) can generally be satisfied by the use of electronic media that provide the same functionality and investor protection as the delivery of paper documents. Documents delivered electronically must be no less complete, timely, comprehensive and confidential than their paper counterparts. The Canadian Securities Administrators' *Delivery of Documents by Electronic Means Policy* provides specific guidance regarding the electronic delivery of documents.

- **Web Site Content:** The Canadian Securities Administrators' *Internet Trading Policy* and the Toronto Stock Exchange's *Electronic Communications Disclosure Guidelines* provide useful guidance regarding the use of Web sites and related media to communicate investor relations information and to effect corporate disclosure. The *Guidelines* caution that information disclosed through Web sites, email, and other electronic media should be viewed as part of the formal corporate disclosure record and is subject to the same laws and rules as traditional forms of disclosure, such as news releases. Among other things, the *Guidelines* recommend that companies establish and implement a clear written policy regarding the use of electronic communications. The *Guidelines* provide helpful and detailed suggestions regarding Web site use, and should be carefully reviewed by all Canadian public companies.

- **Internet Road Shows:** Securities offerings are often promoted through presentations known as "roadshows". Canadian securities regulators do not object in principle to Internet roadshows, provided that they comply with securities laws generally and the specific legal restrictions that apply to traditional roadshows. Regulators have also issued specific guidelines for Internet roadshows.

13

INTERNET RISK MANAGEMENT

This Handbook highlights some of the basic legal and business risks that ought to be addressed in an Internet risk management plan. Organizations should regularly review their business strategies and practices to ensure that they comply with evolving laws and are consistent with business and technical best practices.

The following are some key questions to be considered in assessing an Internet risk management strategy:

- Are you protecting copyright in your Web site content and Internet publications? Do your published works bear appropriate copyright notices, and have you registered your copyright in important publications? Have you used technological measures to prevent unauthorized use of your materials or to assist in the detection and enforcement of copyright infringement?
- Are you protecting your business identity and brands on the Internet? Does your *Web Site Use Agreement* and your *Web Site Linking Agreement* protect your trade-marks? Are you appropriately responding to unauthorized uses of your trade-marks?
- Are your electronic contracts valid and enforceable? Do they comply with applicable electronic commerce laws? Does your electronic records management program comply with electronic evidence laws?

- Do your Web Site and Internet transactions comply with applicable domestic and foreign consumer protection laws?
- Do your Internet advertisements comply with applicable domestic and foreign advertising laws?
- Does your *Web Site Development Agreement* provide you with ownership of your Web site content and underlying software?
- Does your *Web Site Hosting Agreement* provide you with adequate rights and remedies regarding the performance of your Web site?
- Does your *Web Site Use Agreement* adequately protect your interests and has it been effectively implemented?
- Does your *Web Site Privacy Policy* comply with the Canadian *Personal Information Protection and Electronic Documents Act*, provincial privacy laws, and privacy laws of foreign jurisdictions?
- Does your *Communications System Policy* adequately educate employees and others regarding communications system risks, and establish appropriate rules that govern communications system use?
- Do your Internet activities (including your Web site and email communications) comply with applicable securities laws, regulations and guidelines? Have you taken steps to avoid being subject to foreign securities laws?

14

Conclusion

The Internet and related technologies present substantial opportunities, but they also present numerous challenging technical, business and legal issues with significant ramifications for organizations of all sizes and types. Organizations that fail to address those issues in a timely manner may face serious consequences.

As Internet business models evolve and technologies rapidly develop, so too does Internet law. New Internet-specific laws are being enacted, and regulatory guidance and accepted standards and best practices are evolving. Organizations engaged in Internet activities should regularly review their business strategies and risk management practices to ensure that they comply with current laws and regulatory guidance, and are consistent with current business and technical best practices. They should also obtain the benefit of timely legal advice.

The Borden Ladner Gervais LLP Technology Practice Group is experienced in all areas of Internet law, and can provide comprehensive, practical and timely advice. It would be our pleasure to assist you, and we invite you to contact us.

More information regarding the BLG Technology Practice Group is available at *www.blgcanada.com*.

www.blgcanada.com

Borden Ladner Gervais
Lawyers – Patent & Trademark Agents

Calgary
Montreal
Ottawa
Toronto
Vancouver