# *e*-Risky?

***Understanding and Managing Online Legal Risk***

By James Swanson, BASc, LLB, MBA
jswanson@parlee.com
Parlee McLaws
Edmonton, Alberta, Canada


Disclaimer: This paper is written from a very general point of view, primarily from a Canadian perspective, and is merely an overview of selected legal and related business issues. Cyberlaw and the law governing *e*-Commerce are rapidly changing and it is impossible to be current on any issue for long. This paper does not constitute legal advice or business advice and cannot be relied on for any specific situation or set of facts. Some concepts have been generalized and/or simplified and many exceptions to the general rule are not discussed. It is based on the law of the Province of Alberta, Canada and the laws and regulations in force at the time of writing in that province. Those requiring further information or legal advice are urged to contact competent counsel.

---

## 1. INTRODUCTION

As Nicholas Negroponte so aptly put it in his book *Being Digital*, we are undergoing a paradigm shift from moving atoms (i.e. stuff, matter, materials) to moving bits (digital information). Bits are ephemeral and borderless. The Internet was designed to get messages through even in the event of war, so attempts at legal regulation and censorship, being lesser threats, face some difficulties.

Costs can be dramatically cut, small can compete with big, business can be 24/7, and the barriers of space and time can be largely eliminated. On the other hand, competitors can be anywhere, anytime, and may not come from where you expect. Risk management in general becomes more complex.

e-Commerce and e-Business therefore result in an exceedingly complex and fast-evolving area of the law, now known generally as *Cyberlaw*, with the impact of changing technology and business methods creating many new and novel issues and new variations on old ones. It is hoped that the following general comments and items will be useful and informative to anyone engaged in or contemplating an e-Business venture.

## 2. GLOBAL BUSINESS

Going online can mean becoming an exporter and a global business virtually overnight. You're not just running a corner store anymore. You have to decide where (*if you can say such a thing in this context*) you are doing business. Will you accept orders from across the world or just down the street? Just because your web site can be seen by anyone with Internet access no matter where on the planet they are does not mean you have to deal with them, but of course you will at least be tempted. Therefore, you are very likely to now have to deal with not only all the legal issues surrounding international business, but also the social and cultural ramifications.

The appearance of your Web site, your domain name, your language and means of communication, your message and selling proposition, even your trade-marks, packaging and trade dress all become important. Failure to pay attention to these factors can be disastrous.

## 3. JURISDICTION

Jurisdiction is basically the ability of a Court or other Tribunal to assume control, to assert its authority and to enforce its decisions over you. The Internet is global; legal systems generally (excluding things like international treaties) are not. The question therefore becomes what laws do you need to comply with and what ones do not apply. In North America north of the Rio Grande River there are 49 states, 10 provinces, 3 territories and 2 federal governments, all of which are to at least some extent discrete jurisdictions.

It may be said that there are basically 2 types of jurisdiction:

- Prescriptive - this includes criminal law, government regulation and prosecution, control of perceived harmful effects (gambling, pornography, or even manner of dress in the case of some cultures), regulation of medical and professional services, and so on.

- Private International Law - this includes law suits, civil actions and litigation, for such things as breach of contract, torts, infringement, business disputes, etc.

This is a complex area, but the fundamental concept to keep in mind is that foreign courts may validly assume jurisdiction over you, generally on a sliding scale depending on how your Web site is set up, and their assumption of that jurisdiction may be recognized by other jurisdictions, including your own.

Civil liability is particularly problematic. If you are sued in a foreign jurisdiction, you may find that, if you ignore that lawsuit, it may become a judgment which can be registered in your jurisdiction and executed against you (seizing assets or garnishing money, etc.). In fact, there are cases in which lawsuits that could not be brought in a province of Canada directly may be brought in a foreign jurisdiction and then registered and enforced in Canada (this has occurred with gambling debts, for example).

You therefore can't ignore the laws of other jurisdictions. If you are sued, you will need to consider whether to challenge jurisdiction, defend there or ignore, remembering that your defence to a foreign judgment which is sought to be registered here will be very limited. Our courts are not inclined to open up such judgments and let you raise issues here that you could have raised in the first place in the other jurisdiction.

How can you manage all this risk?

First, get good advice on which jurisdictions pose the greatest threat to you legally. Then, you can decide if the rewards of even dealing with individuals or businesses there are worth the risk. You can consider whether you will have any active presence there, or whether you will go so far as to place a notice on your Web site that you do not deal with anyone resident in that jurisdiction.

Secondly, it is possible to enter into a contract by which you and the other parties agree on the law that will apply and the forum (i.e. court system) in which disputes must be decided. This is not a perfect solution by any means, but at the very least, it will give you a defence you would not otherwise have. Web site agreements (which are contracts if done right), while not a complete certainty, can deal with not only which jurisdiction will apply, but other things such as disclaimers and limitations of liability.

## 4. CONTRACTS

Under our legal system, based on English common law, as is the U.S., the U.K. Australia and New Zealand, contracts require three elements: an offer, an acceptance of that offer, and consideration (something of value being exchanged). This is not necessarily the case in other countries as the requirements to form a valid contract vary from one jurisdiction to the next. It is important to consider those requirements when deciding where to do business online and with whom. Further, the comments on managing jurisdictional risk above need to be qualified as the disclaimers, limitations and choice of jurisdiction clauses that are generally enforceable in the common law world may not be in other jurisdictions.

Electronic contracting raises further issues, some of which can be dealt with technically, including:

- Authentication - who sent the message, offer or acceptance?
- Identification - who “signed” or accepted the document or contract?
- Integrity - has the document remained unchanged?
- Repudiation - will the document stand up in Court?
- Electronic Signatures - This can be just the equivalent of an “X”, for example typing a name at the end of an email. Giving it legal effect may be problematic.
- Digital Signatures - Authentication and identification of signor can be accomplished by technical means, which can also verify the integrity of a document and its contents.

There is a lot of new legislation either in force, or coming into force, all across Canada and the U.S. Online businesses need to be up to date on current regulation in the jurisdictions with which they are concerned.

You should also be aware that the United Nations Commission on International Trade Law (UNICTRAL, www.uncitral.org) deals with the United Nations Convention on Contracts for the International Sale of Goods (CISG). Unless disclaimed in a contract for the international sale of goods, the terms of CISG can be implied into the contract. Canada is a signatory to the Convention, so any such sales by you should deal with this issue unless you wish to have CISG apply.

Besides CISG, if you are shipping internationally, you will have to deal with the complex rules of international trade and, even with a domestic shipment, with other matters such as when title passes in a shipment of goods. Possession and title are not the same thing. Usually a Bill of Lading, or similar document, which is actually a contract, will define when title changes. This is important because the entity with title is the one who holds the risk of loss or damage to the goods.

There are some resources out there that can help you as well. The International Chamber of Commerce, at www.iccwbo.org, has the INCOTERMS, which do not have the force of law, but which you can purchase and use in contracts.

Finally, bear in mind that you want to be paid. Granting credit to businesses or individuals in foreign jurisdictions is risky. If they don't pay, you may have an agreement that says you can sue them here, but even if that works for collection of a debt, you will still have to go to the foreign jurisdiction to collect, and that may be expensive as well as difficult or impossible (it's one thing to use a contract as a shield to try and avoid being sued; it's quite another to use it as a sword and seek to enforce your rights).

Credit cards can be a convenient means of assuring payment, but may not equate to money up front. You should be aware that in many jurisdictions, the purchaser can deny the agreement and obligation unless the credit card is physically present at the time of sale. Of course, with e-commerce the card is of course not present, so "charge-backs" can be a problem. In Canada, where the card is not present, the holder of the card has 180 days to charge back the transaction. Rarely, if ever, will the credit card provider side with the merchant. It's therefore fair and reasonably accurate to state that the vendor takes most of the risk in online business.

## 5. MARKETING

There is a body of law surrounding marketing issues, and can be discussed under the heading of the "4 P's of the Marketing Mix. The objectives of marketing law are primarily to protect consumers and the public from harm and unfair selling practices and to foster fair competition.

## 5.1 Product

This will, of course, include a service. There are numerous regulations surrounding product design and packaging, which vary from one country to another. There are also regulations dealing with licenses required to sell, certifications needed to deliver a service, mandatory contractual terms (regardless of what you say in your Web site agreement), cooling off periods in which a customer can just change their without liability, and so on. In addition, there are often voluntary standards that are ignored only at great risk. Businesses should be familiar with all applicable regulations and legislative requirements in the jurisdictions where they conduct business, as well as all applicable voluntary standards.

## 5.2 Promotion

Again, there is a great deal of regulation in this area, as well as voluntary guidelines through many industry associations.

In Canada, the most significant legislation is likely the Competition Act, which regulates acceptable advertising and promotion.

The Competition Act has two approaches:

a) Prohibited Offences - these are criminal in nature (see prescriptive jurisdiction above);
b) Reviewable matters - these are assessed according to a civil onus of proof and can be the subject of an Order by the Competition Tribunal. Many cases are fast tracked. Penalties and published information, retractions and apologies are possible.

The Competition Act prohibits false or misleading advertising and this will apply to Web sites as it does to other media. This includes any representation to the public that is false or misleading in a material respect, and made for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever.

Unfair practices include:

- bait and switch - advertising the cheap stuff (which is not available or is of limited supply) and then upselling;
- targeting groups unfairly (seniors, immigrants, etc);
- selling at prices grossly exceeding the price at which similar goods or services are available;
- calculated and cynical undue pressure; and,
- sale to consumers clearly not able to afford to pay the entire obligation

Other very popular promotion techniques are contests and giveaways. Such tactics are subject to legal regulation. The Competition Act focuses on disclosure of such things as value of prizes, odds of winning and geographic areas. Prizes must be distributed promptly, and winners must be chosen randomly or on the basis of skill. The Criminal Code may require a skill-testing question. A license from the province in which you are located may also be required.

### 5.3 Price

The Competition Act seeks to create a level playing field with respect to such matters as channel power (preventing unfair differential treatment to commercial customers that could severely reduce competition in a marketplace) and prohibits unfair pricing practices, such as:

- pricing conspiracies between competitors;
- price discrimination;
- predatory pricing and dumping;
- price maintenance (controlling pricing further down the channel of distribution);
- bid rigging; and,
- unfair consumer pricing, such as stating the price is lower than the regular price when it is not.

### 5.4 Place

I know that the concept of place can be vague in the Internet context, but by place we mean distribution and such issues as shipping and delivery, sales channels and the manner of sale. Pyramid and multi-level marketing and distribution schemes and channel concepts are common in online business, but it is necessary to understand the legalities before proceeding with any plans in this area.

Is a multi-level plan legal or not? You have to ask yourself the following questions:

- Is there a genuine selling opportunity for those buying distributorships?
- Is the goal of distributorship to sell actual goods and/or services or is it to channel monies back up the chain?
- Is there a realistic opportunity for distributorships to expand?
- Basically, is there a genuine business activity?

Legal schemes are highly regulated and full disclosure is required. Pyramid selling is criminal under the Competition Act if:

- Participants pay money for the right to receive compensation for recruiting;
- Participants are required to buy specific quantity of products other than at cost for purpose of advertising;
- Participants are knowingly sold commercially unreasonable quantities (known as *inventory loading*); or,
- Participants are not allowed to return products on commercially reasonable terms.

There are also illegal discriminatory distribution practices, including:

- Refusal to deal - seller refuses to deal with purchaser even under comparable conditions to purchaser's competitor;
- Exclusive dealing - seller agrees to sell only if purchaser agrees to buy from seller exclusively; and,
- Tied selling - seller will sell only if purchaser agrees to buy other, less desirable goods or services as well.

## 6. INTELLECTUAL PROPERTY

### 6.1 Transfer of Intellectual Property

With respect to how Intellectual Property ("IP") or interests in IP are moved around, it's important to know the following terminology:

- Assignment: This is an outright transfer and sale of ownership, although it may revert back to the seller at some point, or may be a sale of only one of a number of rights in some matter or subject.

- License: This is permission to do something that otherwise would not be lawful. Licenses can be exclusive, non-exclusive, permanent, temporary, irrevocable, revocable, world-wide or restricted in territory, royalty-free or for a fee, etc. With a non-exclusive license, more than one person can receive a license, and the number of persons may be unlimited, depending on the circumstances.

- Waiver: This does not transfer anything, strictly speaking, but is an agreement to not enforce a right that otherwise could be enforced.

### 6.2 Copyright

Copyright deals essentially with the right to copy, and applies to everything from music to literary works to notebooks to drawings to computer code and programs. Any and all rights to copyright are as set out in the Copyright Act of Canada, and in various treaties and conventions to which Canada is a party. There is no common law right.

Original works can be created by old or new technology and digital works, including software, computer code and digital graphics and music are protected. Computer programs originally obtained protection as literary works. Now, a computer program is defined in the Act as "a set of instructions or statements, expressed, fixed, embodied or stored in any manner, that is to be used directly or indirectly in a computer in order to bring about a specific result." Protection can be extended to source and object code, component routines, the screen display that results, and possibly even the programming language itself. Digital graphics, images and logos will be protected as works of art. MIDI and MP3 files will qualify as protected music.

Protection under the Copyright Act is automatic, generally lasting for the life of the author plus 50 years. Only original work is protected. Please note that there is now no legal requirement to use the © symbol to be able to assert copyright. Works that meet the legal requirements are still protected. However, it is generally a good idea to use the symbol to make it clear that copyright is claimed.

Copyright protects expression only. It does not protect ideas, schemes, systems, artistic styles or "any method or principle of manufacture or construction". It cannot be over-stressed that **ideas are not and cannot be protected by copyright**. Copyright prevents copying so infringement usually requires some element of copying.

Registration is optional since every work is protected automatically upon creation. However, registration creates a presumption of validity. Infringement does not require an exact copy, but generally substantial similarity. Generally, in a lawsuit for copyright infringement, evidence of access to the work of the plaintiff and some substantial similarity in the complained-of work of the defendant will have to be proved. Registration may allow for better evidence of that.

Ownership of copyright can be a major issue. Employees creating works for an employer in the course of their employment will find that the employer owns the copyright. However, with freelancers and independent contractors, the copyright will be generally retained by them as the original author unless there is a written agreement transferring ownership of the copyright to the person who hired them to develop or create the work in question.

This is a serious issue in the modern economy. In the information technology and computer industries, the relationship of independent contractors is common. The Copyright Act (Canada) states that transfer of any "proprietary interest" in copyright can only occur if done in writing. Assignments, transfers and exclusive licenses are proprietary interests. Without something in writing, it is likely that all you can receive from an independent contractor (i.e. any non-employee) is a non-exclusive license. The fact that you paid for it will not change that. Many "owners" of Web sites or software or databases or digital graphics may in fact not "own" them at all.

Many computer programs are also compilations of smaller programs, which can make ownership and licensing very complex. Another thing to consider is that copyright in MS Word or PhotoShop goes to the programmer, while copyright in the literary work produced in Word or the image in PhotoShop goes to the writer or creator, not the programmer.

### 6.2(a) Moral Rights

These are separate rights from copyright *per se* and can be enforced legally. In Canada, they last for the same term. Conceptually, an author's work is an extension of the author and should not be subject to attacks on its integrity. There are basically three moral rights: attribution, integrity and association.

The author has the right to have their work attributed to them. An author can choose to remain anonymous, to have their name associated with the work, or even to use a pseudonym, as long as it is "reasonable."

The author's right of integrity protects the author from having the work being "distorted, mutilated or otherwise modified." This applies only if it injures or prejudices the author's reputation, image or honour.

Finally, the author may also have some control over use of the work in "association with a product, service, cause or institution." Again, this is enforceable only if it prejudices the author's honour or reputation.

The Berne Convention also provides for prevention by an author of "derogatory action." In Europe, some legal systems provide authors with a right to prevent excessive criticism of their work. We have no exact equivalent in Canada, although the law of defamation (slander, libel, etc.) might apply.

Moral rights cannot be sold or assigned and can continue in force even though the copyright has been assigned. However, the Copyright Act allows them to be waived. It would be a good idea to have such waivers in writing.

**6.2(b) Copyright Infringement**

With the Internet and digital technology, the costs of copying and distribution of digital property approaches zero. In addition, tracing and identifying the person behind copying and distribution can be difficult or impossible. Even if they can be found, they may be in a foreign jurisdiction where the law is not favourable to enforcing any rights against them.

This is aptly illustrated in the peer to peer ("P2P") phenomenon, starting with such matters as the MP3 format for music and such applications as Napster. Napster facilitated copyright infringement on a large scale using a type of P2P technology but was subject to U.S. jurisdiction (there was a company, individuals and servers physically present in the U.S.). Audiogalaxy was similarly vulnerable to legal action. There are other services that continue to operate, often out of other countries, as of the time of this writing. Further, other P2P technologies, such as Freenet and Gnutella, are not centralized as Napster was and will therefore will be virtually impossible to control.

Technological solutions have been sought, such as the encryption protocol on DVD movie disks. Given the fact that a fifteen year old Norwegian reportedly was able to crack the DVD encryption protocol in three days, technical solutions may not always be effective and are likely always doomed to fail.

Nor should more traditional businesses feel safe. A producer and distributor of ornamental quilt patterns was dismayed to find its products scanned, digitized and being distributed in contravention of copyright via a Web site. *If it can be digitized, it can be Napsterized.*

## 6.3 Trade-marks

Trade-marks are protected both at common law and under the Trade-marks Act. Protection under the Trade-marks Act requires registration at the Canadian Trade-mark Office and is subject to checking and challenge by the Office and by the public, even after registration.

Rights to a trademark do not accrue from mere creation. What does create rights in a trademark is use, or related elements, such as public recognition (linking in the mind of the public between the mark and the product or service) or an intention to use. The rights are not usually those of the creator of the trademark, but of the person behind the use, intent or creation of public recognition.

Besides registration, there is common law protection. To protect unregistered trademarks, we have the action of passing off, which is used to stop use of a confusing similar or identical mark with the result of damaging the business of another. To win a passing off action, a party must prove:

a) reputation or good will acquired in a business, name, mark or other trading symbol;
b) a misrepresentation by the defendant causing confusion or deception between the two businesses;
c) actual or likely damage;
d) no public policy reason to not grant a remedy

Attributes of a Trade-mark:

a) Has to have a Mark – "any sign, or combination of signs….including personal names, designs, letters, numerals, colors, figurative elements." Slogans ("let your fingers do the walking") have qualified.
b) Must be distinctive (not merely descriptive) and actually distinguish one business's products or services from another's, or be capable of being "adapted to distinguish" them.

It's notable that a trademark can lose its distinctiveness by falling into the language as a general term. "Nylon" was once a trademark. "Thermos" almost lost protection in the 1960's when the public began to use the term for any product of that type. The courts in both Canada and the U.S. considered the thermos matter and ruled that a sufficient minority of consumers still linked it with the product. The courts in the U.S. also allowed competitors to use the word "thermos", but without the capital "T", as long as they added their own brand name and did not use works such as "original" or "genuine."

If a trademark is used simultaneously in Canada by two businesses, it cannot be said to be distinctive, and neither can register. If this happens after registration, the registered mark can become invalid if nothing is done to enforce the registrant's rights. As a result, companies can

be very vigilant and aggressive in defending their trademarks to avoid losing protection, and that aggression extends to using their trade-mark in a domain name.

### 6.4 Domain Names

At the same time, domain names and trade-marks have been colliding head on in what can be summarized as:

**.com v. TM**

Remember, domain names are global and alphanumerically unique. There can be only one swanson.com or swanson.ca (*and I don't have either of them*).

Trademarks are generally regional and at most national, unless they have become nearly global by long standing and wide spread use, or registration in many countries, or both, such as the Coca Cola's and McDonald's of the world. There can be many businesses using the name Western – Western Trucking, Western Booksellers, Western Wholesale, etc., and the identical name can coexist in different geographical markets. However, there can be only one western.com, which of course leads to friction as the demand for the best domain names increases.

Domain names are not really property in the usual sense but are actually contracts for provision of a service.

Each particular generic top level domain name, ("GTLD"), or extension, such as ".com" or ".ca" will be administered by a particular body, and its specific rules will apply. For example, ".com is largely under the control of ICANN and Verisign in the United States while ".ca" is run by CIRA, the Canadian Internet Registration Authority. Anyone anywhere on earth can register a ".com", while ".ca" is essentially limited to Canadian content.

This means that the trade-mark law of the United States is not particularly likely to apply to a ".ca" domain, while it is very likely to be applied to a ".com", even if the registrant of the domain is not in the United States. An American trade-mark holder will find it much easier to attack the registration and use of a ".com" domain by a foreigner under traditional theories of trade-mark law than would be the case if the foreigner used a domain not subject to U.S. presence and control. This will be so even if the foreigner has a valid trade-mark in the other jurisdictionfor the same word as the disputed domain.

You will therefore want to be careful that your domain name is not subject to third party trade-mark infringement claims, and you will likewise want to be sure that your trade-mark is not being diluted by use by someone else in their domain name. The world has truly become smaller, and it's more important to think internationally in terms of names for businesses, products and services.

## 6.5 Patents

Patents protect inventions, and are issued solely under the Patent Act. Unlike trademarks, there is no protection at common law. "Inventions" are "any new and useful art, process, machine, manufacture or composition of matter, or any new and useful improvement in any art, process, machine, manufacture or composition of matter. The intention is to encourage creativity and the development of new technologies. Therefore, to achieve protection, an idea needs to be:

a) new
b) useful
c) non-obvious

A patent can be granted to the inventor (or the employer of the inventor in some cases) for new, useful and non-obvious ideas with practical industrial application. The patent system forces the inventor to fully disclose so that others may work to improve the idea, and rewards this disclosure with generally an absolute monopoly for the period of the patent. It's important to note that patent laws vary from one country to another, and what may be patentable in one country may not be in another.

Generally, patents now last 20 years from the date of filing the application. The first to file an application may win any dispute. Accordingly, it is important to protect the idea by keeping it as confidential as possible until the application has been filed.

The holder of the patent is granted an absolute monopoly for the period of the patent. Nobody can sell or use the invention, even if they arrive at it independently without knowledge of the patent. Of course, the patent may be licensed to one or many parties. The holder of the patent must pay annual maintenance fees ($100.00 rising to $400.00 annually).

It's important to note that there is no such thing as an international patent – applications are made country by country.

Patents have become a trendy area in e-Commerce. The United States has been ready to grant patents for business and technological processes, while the European Union has excluded much of the same area from patent protection. There are many cases in litigation in the U.S. so how e-commerce and business process patents will sort themselves out in the long run is not certain.

For now, online businesses need to consider whether their conduct infringes someone's patents in a manner in which they could become subject to jurisdiction and enforcement and, at the same time, there is a need to consider whether your online business has something that could be protected and exploited by the strategic use of patent law.

## 6.6 Trade Secrets

A Trade Secret is any information or item or body of knowledge that gives its owner a commercial advantage over others. The advantage derives from the fact that it is not generally known. The advantage exists only as long as that remains the case.

Unlike the situation in the U.S., there is no specific Canadian legislation dealing with Trade Secrets. In 1986 the Alberta Law Commission did prepare a report in the area, including a draft Trade Secrets Act, which has not been enacted, and which included the following definition:

> "Trade Secret" means information including but not limited to a formula, pattern, compilation, programme, method, technique, or process, or information contained or embodied in a product, device or mechanism which:
>
> i) is, or may be used in a business,
> ii) is not generally known in that trade or business,
> iii) has economic value from not being generally known, and
> iv) is the subject of efforts that are reasonable in the circumstances to maintain its secrecy.

If your confidence is breached, and your trade secret is disclosed, you may be able to pursue a remedy in the courts by suing the parties who breached the confidence and possibly the recipients of the information, depending on the circumstances, as well. Innocent purchasers from an industrial spy are less likely to be held liable than someone who participated more or less actively in a plan to steal the information.

In order to succeed, you will likely need to fit your case within the following parameters:

a) Your information was in fact a trade secret, and you took reasonable steps to maintain its secrecy. This might include things such as locking it up, keeping it in a restricted area, limiting access to it, etc.
b) If your information was previously disclosed, it was done under circumstances which led to an obligation of confidentiality arising. For example, was it revealed only to those employees who needed to know to perform their duties? Did the recipients of prior disclosure sign confidentiality or non-disclosure or secrecy agreements?
c) Has a party used or misused the information so that you have suffered damage? You likely cannot sue someone for simply having learned the secret – they must have done something such as use it in a manner which damages you economically.

Trade secrets may also be subject to other forms of legal protection. A customer list might be subject to copyright. A secret device or process might be patentable.

Trade secrets have some distinct advantages. They can theoretically last forever, while things like patent and copyright expire. They may be enforceable in many jurisdictions without registering a patent in each.

On the other hand, the primary problem is this form of protection can be lost no matter how hard you try. The law requires that you make all efforts possible to maintain the secrecy, and this will mean adequate network and computer security.

Others may innocently and independently come up with the same idea. Or, it may be reverse-engineered but then changed or improved to the point that it is no longer an infringement. A patent could prevent much or all of that – a trade secret will not.

Publication or disclosure destroys the value of a trade secret. Lawsuits for infringement or disclosure may not lead to a satisfactory result, particularly where the defendant can't be found, or the defendant may be judgment proof, having no assets to pay or being in a jurisdiction where they cannot be attacked. Even where damages can be collected, they can be a very inadequate remedy. Of course, once the secret is out, an injunction forbidding the disclosure is often neither possible nor, if granted, effective.

To fully protect yourself in any situation, you should use a properly drafted and executed non-disclosure, confidentiality or secrecy agreement (all pretty much the same thing). Such an agreement will not only define the rights and obligations of the recipient of the disclosure, but also of you. Further, it will serve as evidence of the efforts made to keep the information secret, which will be required in any circumstance where a dispute ends up in court. Finally, such agreements are for people you already trust.

## 7. SECURITY

Security is obviously a key issue in online business. As holes are patched and viruses and other exploits become known, new threats pop up. Security is therefore truly a process and not something you just set up and leave.

Loss of security in terms of customer information can be a disaster. Online businesses make the best trophies for hackers and therefore are often high profile targets.

While a full discussion of security is beyond the scope of this paper, managers of online business must keep in mind that loss of security can mean loss of customer confidence, loss of prestige, loss of competitive advantage, breach of legal obligations and statutory or regulatory requirements, and can even end the existence of the business.

In addition, loss of security can lead to loss of protection of trade secrets (see above) and other valuable but intangible intellectual property, assets and information.

Online businesses need to know and assess their security risks and take appropriate steps to manage them. This can include not only technical steps, but being pro-active legally as well, being careful to disclaim liability due to breaches of security and to not promise to deliver more than you can if a security issue gets in your way.

## 8. PRIVACY

A key issue in e-business, and one closely related to security, is privacy. Just what is it? A commonly cited definition is as follows:

- the right to control intrusion into a person's seclusion;
- the right to control disclosure of private facts about a person;
- the right to prevent a person being put into a false light in the public eye; and,
- the right to control the exploitation of a person's name and image

Different jurisdictions have taken different approaches to privacy legislation. These range from the U.S. which is largely laissez faire, to the European Union, which in 1998 passed its Privacy Directive, which provides, among other things, that European companies may not share personal information concerning individuals with companies in other jurisdictions, unless those jurisdictions have similar laws.

The Canadian approach is the Personal Information Protection and Electronic Documents Act, or PIPEDA, which deals with a number of areas of concern such as privacy and security in on-line matters. PIPEDA establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities, in connection with the operation of a federal work, undertaking or business or inter-provincially or internationally and ultimately, as of January 1, 2004, will apply to commercial transactions within a province of Canada as well. If you are collecting or holding information from individuals, you should be aware of the implications as the legislation comes into effect.

PIPEDA provides for the Privacy Commissioner of Canada (www.privcom.gc.ca) to receive complaints concerning contraventions of the principles of privacy protection required by the Act, to conduct investigations, to conduct audits and to attempt to resolve such complaints. The audit provision is significant – an audit can include entering a place of business, compelling production of documents and requiring witnesses to testify under oath.

Unresolved disputes relating to certain matters can be taken to the Federal Court of Canada for resolution. The Court can order damages, including punitive damages or damages for humiliation, and can force publication of public apologies. There are also penalties for firing or harassing whistle blowers, obstructing investigations or audits, and destroying information which is the subject of a request. The maximum fine is $100,000.00.

Personal information includes information in basically any form which could identify a person or be connected to a person, including name, age, income, ethnicity, blood type, credit records, medical records, disputes, any ID number or similar identifier, and will include any personal information included in such things as evaluations, disciplinary proceedings and actions, opinions, comments, and so on.

Commercial activity that falls under PIPEDA includes almost any conduct, dealings or transactions of a commercial nature, and will include the selling, bartering, sharing of membership or donor lists, so even fundraising activities are caught.

PIPEDA generally follows the CSA Model Code for the protection of personal information and establishes the following 10 principles to govern the collection, use and disclosure of personal information. In summary fashion, the following are the principles:

1. Accountability – A business ("business" means any person, organization or entity caught by the Act) must appoint a privacy officer responsible for compliance with the Act and make contact information for that person publicly accessible. The officer will be responsible for protecting all personal information held by the organization or subject to transfer to a third party.

2. Identifying the purposes for the collection of personal information – Businesses must identify the reasons for collecting personal information at or before the time of collection. They must document why the information is collected, inform the individual from whom the information is collected why the information is needed, and ensure that the purposes are limited to what a reasonable person would expect under the circumstances.

3. Obtaining consent – Consent must be obtained before or at the time of collection and must be obtained again whenever a new use for the personal information is identified. It is notable that consent may not be made a condition for the supply of a product or service, unless the information is actually required to provide the product or service. Generally, the consent will have to be express and not implied. However, in the case of non-sensitive data, reasonable expectations of the donor may be used in determining whether their consent may be implied.

4. Limiting collection – Personal information can only be collected to the extent necessary for the identified and stated purposes.

5. Limiting use, disclosure and retention – Businesses must put guidelines and procedures into place for how they use, disclose and retain personal information. This will include instituting maximum and minimum retention periods and disclosing those. It must also take into account legal requirements or restrictions and mechanisms for redress. Destroying information that is no longer needed must be done in a way that prevents improper access to that information. Technologies such as shredding and electronic erasures will be required.

6. Ensuring and maintaining accuracy – Businesses are made responsible to minimize any possibility of using incorrect personal information through adopting such techniques as checklists that list specific items of information required to provide a product or a service. Records must be kept of the location or locations where all related personal information can be retrieved, of when the personal information was obtained or updated and of the steps taken to verify the accuracy, completeness and timeliness of the information.

7. Providing adequate security – Adequate measures must be taken to be certain that personal information is protected against loss or theft, unauthorized access, disclosure, copying, use or modification. This will require design and implementation of a company security policy that includes appropriate technological, physical and organizational security and controls. This does not just refer to computer and network security, although that will be key; it also will refer to security

with respect to physical premises (where the computers may be located, of course) and with respect to which persons in an organization should have access to information and what sorts of non-disclosure requirements might need to be in place.

8. Making information management policies readily available – This is basically *openness*. Businesses must make their privacy policies and practices both easily available and understandable. This includes, as noted above, appointing a privacy officer and publicly stating the means for contacting that person.

9. Providing individuals with access to information about themselves – The general rule is that individuals are to have access to all information held by a business about them at no cost, or at most minimal cost, within 30 days of request, unless the information comes under a statutory exceptions under the Act, which includes information covered by the privilege between a lawyer and his or her client, information disclosed to law enforcement, cases where disclosure could harm an individual's security or life, and confidential business or commercial information in certain cases.

10. Giving individuals a right to challenge compliance – Businesses subject to the Act must develop simple and easily accessible complaint procedures. They must investigate all complaints received, and they must take appropriate measures to correct information handling practices and policies in light of complaints.

This creates, or will create, a whole new layer of bureaucracy in many organizations.

### 8.1 Privacy Policies on Web Sites

You need to fully understand how your Web site is affected. If your Web site collects personal information, whether by asking for phone numbers, addresses, etc. or even if it's just email addresses or the use of cookies to track visitors, you should definitely create a privacy statement allowing visitors and customers to determine your policies in a public and accessible manner. Online profiling and "click-streaming" will be likely be subject to PIPEDA.

A privacy statement will make it clear to those reading it precisely what you do and do not do with information collected, which may have benefits outside the realm of legal compliance. Without such a statement, you may lose prospective customers. A properly drafted privacy policy and statement may not only minimize your legal exposure, it can serve a marketing function as well, allowing you to attract and retain customers who otherwise might not be as inclined to deal with you.

Whatever you do, do not create a policy and then not follow it precisely. This is an invitation to disaster, including not only possible legal problems, but also injury to your reputation and goodwill.

It is therefore important to not just let the policy sit once it has been posted. It should be revisited regularly to determine whether or not it is still accurate and to evaluate whether or not it might be revised to assist you in obtaining business goals and objectives.

### 8.2 P3P

In addition, beware of privacy issues costing you customers and money. For example, P3P, or the Platform for Privacy Preferences, now allows web sites to encode their privacy practices in a manner which browsers such as IE version 6 can read. If a visitor to your site has configured her browser to reject your configuration, they may receive error or time out messages. They may not be aware as to why they can no longer log in. You may not be aware that you've lost them. I personally had a time out experience with the Web site for a major airline, a site I had been using for a long time. It occurred to me it might be my recently installed IE 6 so I checked and found that was the problem. My email to the airline was never acknowledged; I thought the marketing tip was worth a couple of free tickets somewhere nice, at the very least.

## 9. INTERNET SPECIFIC ISSUES

This area includes some of the "sexy" topics, like cybersquatting, linking, framing and so on.

### 9.1 Cybersquatting

This occurs when someone registers a domain name which is either the trade-mark of another, or similar to it. This is done in what is often referred to as "bad faith", without any valid proprietary claim but in the hopes that the trade-mark holder can be held to ransom and will pay dearly for the domain.

This worked for a while, but now it will just get you sued. In the U.S. the Lanham Act and the Anti-Cybersquatting Consumer Protection Act (1999) have been used to successfully squash many such attempts. Various domain administrators have dispute resolution policies which can be used to force online arbitrations to quickly resolve such disputes.

See for example, the ICANN UDRP at http://www.icann.org/udrp/ or the CIRA CDRP (Canadian Dispute Resolution Policy) at http://www.cira.ca/en/cat_dpr_policy.html.

### 9.2 Linking

Linking *per se* is what the Web was designed to do, and in most cases, it will be perfectly legal, even without permission of the other Web site or URL.

### 9.3 Deep Linking

If you link deep into another Web site, bypassing its opening views and revenue-generating advertising contained there, you may find that you are legally liable for doing so, as there have been cases in this area.

### 9.4 Framing

Framing another Web site may be copyright infringement, trade-mark infringement or unfair competition. In the famous *Washington Post* case, totalnews.com was allegedly framing Washington Post news content as its own, and selling advertising. The *Washington Post* was successful in stopping that practice.

### 9.5 Meta-tags

These are hidden words in the code to Web sites which are used by some search engines to index and find sites. Use of a trade-mark belonging to another may be infringing and illegal. For example, many sites using the word "playboy" to attract traffic have found themselves in court with the owners of the well-known magazine.

### 9.6 Interference with Traffic

Practices such as Page Jacking (essentially taking another site, usually a competitors, making a copy of it, submitting it to search engines so that it is indexed and then replacing it with your own), search engine keying (paying for higher results on certain words) and numerous other ways of manipulating search engines may or may not be illegal. It's important to understand that, just because technically you can do something, that does not mean that it will be legal.

## 10. OTHER ISSUES

Being an online business does not make you exempt from other areas of the law, but the global nature of the Internet, and the way in which the technologies work, do lead to other interesting issues and areas of concern, including, for example, the following (which are just selections from a rapidly changing list):

- Securities - offering shares in a company to the public and related matters are highly regulated. Doing so online means you must consider jurisdictional and regulatory issues. Offering shares in your company to the public must be done in compliance with all applicable laws, and usually requires advance approval.

- Taxation - the OECD model tax treaty requires a permanent establishment and/or core business activities, as contrasted to a preparatory or auxiliary function, before profit can be attributed and therefore tax applied. Other related issues include:
    - Is it a good or a service?
    - Is it exported?
    - Is it delivered here?
    - Is it delivered or provided somewhere else?

- Torts - civil wrongs giving the right to sue, which can include libel ("cyberlibel"), slander, defamation, negligence, breach of confidence, fraud, deceit, identity theft,

inducing breach of contract, interference with advantageous economic relations, and on and on.

- Evidence - when all the documents are digital, some unique issues arise, including recovery of materials thought deleted, difficulty in authenticating the origin, author and version of a record, etc.

- Insurance coverage - is it available?

## 11. CONCLUSION

### 11.1 Food for Thought

- Plan for success – otherwise, you may just be headed for failure.

- Customer loyalty on the Web is generally non-existent and always fleeting. You may not have a second chance to do it right.

- Make sure you own your intellectual property rights and that you are not infringing on the rights of others.

- Understand that *e*-Business may make you an instant exporter. If so, be sure you get advice on the rules governing your situation. Your Web site will be open to the world, with its myriad of jurisdictions, languages and cultures. Cross-cultural issues are crucial.

- Keep in mind that the fundamentals of business in the real world are still as significant as ever. And most definitely, don't think that going into business on-line is an easy way to riches. If you don't have a good understanding of the fundamentals of business in general, and a further good understanding of the unique aspects of on-line business, you may well find that your business fails.

- It may not be rocket science, but *e*-Commerce is not simple either, and certainly not for those who do not understand it. If you have questions, or are unsure, get expert advice. Find and rely on good partners, consultants and providers – technical, marketing, strategic, financial, legal, operational, etc.

- Don't get an "F" in "e"-Commerce – get it right the first time.