

# **ELECTRONIC COMMERCE: “CUTTING EDGE” CHANGES AND CHALLENGES TO COMMERCIAL LAW AND PRACTICE**

Amy-Lynne Williams\*

## **Introduction**

As little as five years ago, if you were a general commercial lawyer who acted for companies that did business globally — you knew what they were up to. There were offices to open in the United States or abroad, staff to hire, international taxation issues to be explored, agreements to review and adapt to foreign jurisdictions and a myriad of additional international issues to review. If your firm could not handle it all, you either brought in another local firm or hired counsel in the other countries.

Many lawyers knew that this was not their strong suit and so did not even attempt this work. But as we all know, “times have changed”.

As a general commercial lawyer in the late 1990s, it is possible for almost every one of your clients to do business in an international arena with the click of a button — on their web site. Companies that would never before have had the capital and personnel necessary to carry out an international expansion, now just need to set up a web site and they have the potential to sell their goods and services to a world-wide market. Sometimes you may not even know it has happened!

More than 300 years of law in Canada, United States and England define the rules that apply to commercial relationships and we are all comfortable with them. These rules rely heavily on the exchange of paper records documenting transactions. Specific statutes and judicial decisions give certainty that business agreements can be enforced, if they are reduced to writing. Rules of evidence largely favour written documents as proof of legal obligations. Consumer protection laws require written disclosure of contract terms and acknowledgment of those terms by a written signature. Intellectual property laws, while developed to protect intangible rights, also rely on written documents to establish and evidence property rights.

All this is changing.

---

\* Partner, Deeth Williams Wall, Toronto, Ontario. This is the text of the Pitblado Lecture, delivered at the University of Manitoba.

With the ease of carrying on business internationally in cyberspace, comes a host of new issues for commercial lawyers to tackle. It is no longer an area that can be ignored if you want to provide professional, value-added legal services to your clients.

This paper will look briefly at some of the questions that will need to be answered for your clients who wish to do business on the Internet and in an electronic environment, as well as some of the changes to general commercial law that have to be made to keep up.

Clients should however, be made to understand that the planning that goes into the traditional set up of a "physical" global business need to also be brought to bear in launching a "virtual" global business in order to take advantage of the world of electronic commerce.

### **Some Questions to Ponder**

1. What is the position of the courts on the enforceability of supply and license agreements that are entered into on-line?
2. What disclaimers should your client place on its web site with respect to implied warranties and conditions? What do they have to do to make them effective and enforceable?
3. What will be the governing law of the agreements your client enters into? Can they choose?
4. Can your client advertise their products worldwide? What risks do they run?
5. Will the electronic records prepared by your client in the course of operating the business be admissible as evidence?
6. What about copyright infringement and the use of your client's trademarks on the Internet?
7. What are your client's obligations with respect to personal or credit information that may be collected in the course of making sales over the Internet?
8. How will contract and product performance disputes be resolved? What if your client is in Winnipeg and the customer purchased products from the web site while living in California?

### **Other General Issues to Consider**

1. Does your client need to register to do business in other countries?
2. Will your client's on-line business be subject to regulation in other countries?
3. Will your client's business even be legal in all countries?
4. Has your client arranged for a customs agent to handle the realities of having to ship goods around the world? Do they know what the export restrictions are for the products they are selling?

5. What is the responsibility of your client to collect and remit GST, PST or consumption taxes on sales conducted over the Internet?
6. How do the traditional concepts of "permanent residence", "residence" and jurisdiction for tax purposes apply to your client and its customers?

## **Contracts**

What is the position of the courts on the enforceability of supply and license agreements that are entered into on-line?

The answer to this question probably will depend on how clear the terms of the agreement are; how they are brought to the attention of the customer; when they are brought to their attention; and whether the system tracks and stores a record of whether the customer actually agreed to the terms. Can your client prove that the customer agreed to the terms of the contract before the sale was completed?

A recent U.S. decision has held that the defendant was bound by Terms of Service posted on a web site as a result of clicking on the "I agree" button and may provide some guidance to the steps that need to be taken by vendors and service providers to ensure that their online contracts can be enforced.

### *Offer and Acceptance*

As in all contracts, there must of course be an offer, acceptance and communication of that acceptance.<sup>1</sup> In an on-line environment, however, it may not always be apparent which party is making an offer and which one is accepting. For example, an offer may be made when someone enters his or her name in an electronic order form on an Internet home page. In this instance, acceptance of the offer probably occurs when the Internet service provider receives the offer and processes the order. If the customer is offering to pay with a credit card, acceptance of the offer may be given only when the credit card company has authorized the transaction.

The final step in forming the contract is communicating that acceptance back to the offeror. The contract is complete only when the offeror receives confirmation that the offer has been accepted. Until that point, the offer may be withdrawn.

---

<sup>1</sup> See, generally, S.M. Waddams, *The Law of Contracts* 3d ed. (Toronto: Canada Law Book Inc., 1993)

In a store, acceptance is communicated instantly at the cash register, by receiving payment and handing over the goods. When it comes to various forms of electronic communication, the law is far less certain.

In a U. S. case, an “order tracking number” issued by an automated telephone ordering system was found to be merely an acknowledgment of the order, rather than an acceptance which formed a binding contract. The result, in that case, was that the customer who placed a large order the day before a major price increase was forced to pay the higher price because the supplier was not bound by its automated acknowledgment.<sup>2</sup>

Understanding the sequence of offer and acceptance is important, not only to determine when a contract has been completed, but also to determine where it is made. Generally, in the absence of an agreement to the contrary, the law of the jurisdiction where the contract is concluded (the location of the accepting party) will govern the contract. In an electronic commerce environment, where a seller may be dealing with potential buyers from around the world, it may be advantageous for the seller to control the jurisdiction of the contract. By selecting a favorable jurisdiction, the seller may be able to exclude or limit implied warranties and to limit its liability.

### *Writing Requirements*

Under Canadian law, most commercial contracts need not take any particular form in order to be enforceable. However, written agreements carry more weight in court if there is a disagreement over contract terms. Electronic communications between the parties may satisfy the writing requirement, but only if the parties clearly intend them to do so.

Some statutes expressly require contracts to be “in writing” or to be accompanied by a “signature” to be valid. This will continue to be relevant in electronic commerce, perhaps even more so, since buyers may have even less opportunity to judge the reputability of on-line sellers.

---

<sup>2</sup> *Corinthian Pharmaceutical Systems Inc. v. Lederle Laboratories* (1989) 724 F. Supp. 605 (S.D. Ind.)

### *Interpretation Act*

A number of statutes expressly require that agreements be "in writing", but few define what that means. The *Ontario Interpretation Act*<sup>3</sup> and similar statutes in other provinces define writing as something "printed, painted, engraved, lithographed, photographed, or represented or reproduced by any other mode in a visible form."<sup>4</sup> The common element, it seems, is an element of permanence. So, while a display on a computer screen may be "in a visible form", concerns regarding the ease with which such data may be altered may prevent a screen display from being sufficient to satisfy this requirement, without a "hard copy" printout or permanent electronic copy of the information.

Although electronic records are regularly accepted in evidence, the security and audit features of the electronic system must be demonstrated, in order to convince the court that such records are reliable. Current advances in the use of cryptography to produce "digital signatures" may go a long way toward establishing the authenticity and reliability of electronic communications.

### *Sale of Goods Act*

Most provinces have legislation governing the sale of goods. In Ontario, the *Sale of Goods Act* was amended to repeal section 5 of the Act, which previously required certain contracts to be in writing. The explanatory notes to the amending legislation state that the change "will reduce the uncertainty of contracts made by electronic data interchange and will allow the public and private sectors to dispense with costly paper backup of these contracts."<sup>5</sup>

### *Statute of Frauds*

This statute states that certain contracts are not enforceable, unless they are in writing. Section 4 of the Statute, which has been adopted by legislation or judicial decision in most provinces,<sup>6</sup> among other things, requires any contract which is not fully performed within one year to be evidenced by a written memorandum, signed by the party against

---

<sup>3</sup> R.S.O. 1990, c. I-11.

<sup>4</sup> *Ibid.* section 1.

<sup>5</sup> Bill 175, *An Act to Amend the Statutes of Ontario*, section 54. The act received Royal Assent on December 4, 1994

<sup>6</sup> R.S.O. 1990 c. S-19; statutes are also in force in New Brunswick, Nova Scotia and Prince Edward Island; equivalent rules have been adopted by the courts in Alberta and B.C.

whom the contract is to be enforced. That portion of the section has also been repealed in Ontario,<sup>7</sup> but remains in force in other provinces.

### *Consumer Protection*

The Ontario *Consumer Protection Act*<sup>8</sup> requires that all “executory contracts” contain specified information and be in writing. Such contracts are not binding unless they are “signed” by each of the parties and a duplicate original of the contract is in the hands of each party. An executory contract is defined as “a contract between a buyer and a seller for the purchase and sale of goods or services in respect of which delivery of the goods or services or payment in full of the consideration is not made at the time the contract is not entered into.”<sup>9</sup>

These provisions of the Act are not affected by the repeal of the provisions of the *Sale of Goods Act* and the *Statute of Frauds* referred to above. Accordingly, most electronic transactions involving consumers will be subject to the Act, unless the products or services involved are immediately delivered on-line.

Similar consumer protection laws have been enacted in most jurisdictions, to protect the public from unscrupulous sales tactics. Although on the surface, the same concerns would appear not to apply to transactions on the Internet, where buyers must seek out sellers, legislators may perceive a need to protect consumers from false and misleading sales pitches in the electronic marketplace. Leaving aside the virtual impossibility of enforcing such laws, one may argue that even the attempt to do so could present an insurmountable obstacle to consumer use of electronic commerce.

### **Liability**

What disclaimers should your client place on its web site with respect to implied warranties and conditions? What do they have to do to make them effective and enforceable?

Certainly, suppliers need to place all disclaimers of liability in a conspicuous place on their web site, preferably linked to all other pages on the site so that the disclaimer does not get by-passed if the consumer links to other pages. The same rules that apply to disclaimers in written, paper contracts apply to electronic contracts as well. They must be clear, be brought to the attention of the consumer and provide notice to the

---

<sup>7</sup> Bill 175, *An Act to Amend the Statutes of Ontario*, section 55.

<sup>8</sup> R.S.O. 1990, c. C-31.

<sup>9</sup> *Ibid.*, section 1.

consumer prior to the time the contract is fully performed. In an electronic setting, it is important for the customer's acceptance of the terms of the disclaimer to be unambiguous and the site should keep track of whether a particular customer agreed to the terms or not.

## Jurisdiction

What will be the governing law of the agreements your clients enter into? Can they choose?

One of the risks an online client can face is the possibility of suits from multiple jurisdictions. Some U.S. jurisdictions are trying to force web site owners to conform to certain consumer protection rules and there is a temptation for any government to extend the reach of "long arm" statutes to try to cover the activities of foreign web site owners who happen to venture into their territory through the operation of their site.<sup>10</sup> The rules of private international law and conflict of laws that apply in Canada have generally been developed on the basis of geographic sovereignty over persons and their acts. These rules are difficult to apply to electronic commerce transactions which have no physical manifestations within a territory and which can easily be structured to avoid geo-political boundaries. In many cases, the multi-jurisdictional aspects of a transaction may be entirely inadvertent. For example, a supplier of goods or services over the Internet or other similar network may not know where its customers are physically located. Similarly, the person receiving the products and services may be unable to determine where they originate.

Issues of capacity to contract, contract formation, formal validity, scope of implied or express obligations, illegality and public policy, enforceability and remedies may all depend on the governing jurisdiction. The parties to an electronic contract must also give thought to the appropriate jurisdiction and the procedural rules for hearing any disputes. The parties to an electronic transaction may determine some of these issues by agreement. Generally speaking, choice of law and jurisdiction clauses in a contract are enforceable in the courts of Canada. However, there may be specific circumstances, such as fundamental breach or unconscionability, which would cause the courts to reject such a clause.

In the absence of an express agreement between the parties regarding the applicable jurisdiction, there are a number of instances in which the Canadian courts will take jurisdiction. A court may have jurisdiction *in rem* or *in personam*. In a contract dispute, a court of a Canadian province will have jurisdiction over the subject matter of the contract (*in rem*) if the contract was formed in that province or if the contract is to be

---

<sup>10</sup> See for example, S.17538 of the California Business and Professions Code

substantially performed within the province. In addition, the court may have jurisdiction over one or more parties to the contract (*in personam*) if the party is resident in the province, carries on business there or has some other “substantial connection” to the jurisdiction.

The Supreme Court of Canada has stated that in tort cases, there must be a “real and substantial connection” between the jurisdiction and the wrongdoing.<sup>11</sup> Where the case is based on negligent or fraudulent misrepresentation, the courts of the location where the statements were received and relied upon have jurisdiction.<sup>12</sup>

In defamation cases, the Ontario courts have held that the place where the defamatory statements were published or disseminated is the proper jurisdiction.<sup>13</sup>

The Supreme Court of Canada has recently stated that the law of the place where the activity occurred is the proper law to apply.<sup>14</sup> However the court also recognized that there are situations where the harm caused by an act may occur in another jurisdiction, or in several other jurisdictions. In those cases, the court has said, other considerations may govern and it may be sufficient simply that a significant portion of the activities were conducted in Canada or a substantial part of the harm was suffered in Canada.<sup>15</sup>

Both the common and civil law jurisdictions in Canada permit legal action to be commenced against a non-resident if the contract in dispute was made in that province. There do not appear to be any reported cases in Canada which have directly considered the jurisdictional and conflict of law issues relating to electronic commerce or the Internet. Clearly, electronic communications can be received or have an effect in several jurisdictions. In the case of statements made over a computer network (for example, misrepresentations made with respect to a product or service), the statements may be received and relied upon by a number of persons in several locations. Defamatory statements may be published globally with the push of a button. Contracts may be breached or other harm inflicted on persons in remote locations.

Can a disclaimer be used to limit the forum to which all disputes are to be referred so that your client is not exposed to unlimited jurisdictions? A recent U.S. case appears

---

<sup>11</sup> *Moran v. Pyle National (Canada) Ltd.*, [1975] 1 S.C.R. 393

<sup>12</sup> *National Bank of Canada v. Clifford Chance* (1996), 30 O.R. (3d) 746 (Ont. Gen. Div.)

<sup>13</sup> *Jenner v. Sun Oil Co. Ltd.*, [1952] O.R. 240 (Ont. H.C.)

<sup>14</sup> *Tolofson v. Jensen*, [1994] 3 S.C.R. 1022

<sup>15</sup> See for example, *Libman v. R.*, [1985] 2 S.C.R. 178; in an intellectual property context, see *CAPAC v. Good Music, Inc.*, [1963] S.C.R. 136



to indicate that it can if properly worded.<sup>16</sup> The issue of the jurisdiction of the contract and the governing law is not only important in the event of a dispute with a customer, it may also keep the supplier from having to fight battles all over the world and perhaps even keep it from facing regulatory challenges in other venues.

## Advertising

Can your clients advertise their products worldwide? What risks do they run?

Misleading advertising of either goods or services "by any means whatsoever" is a criminal offense under the federal *Competition Act*.<sup>17</sup> In order to constitute misleading advertising under the Act, there must be a material and misleading representation made to the public for the purpose of promoting, directly or indirectly, the supply or use of a product, or a business interest. The representation must also concern the price at which the products have been, were or will ordinarily be sold.<sup>18</sup>

Although there have been no cases on the point to date, the wording of the misleading advertising provisions would probably include electronic communications through the Internet. The misleading advertising provisions also deem importers responsible for the offence where it is committed outside of Canada.<sup>19</sup>

Because misleading advertising is a criminal offense and the Crown must prove intent to mislead, it has proven to be relatively difficult to secure a conviction under the *Competition Act*. It has been suggested that the provisions would be more effective if they were dealt through the mechanism of administrative complaints to the Competition Tribunal. The Director of Investigation and Research of the Bureau of Competition Policy recently proposed the creation of a dual civil and criminal system of sanctions for misleading advertising. The majority of the cases would be dealt with under the civil provisions, while criminal sanctions would be reserved for the more flagrant ones.

Provincial consumer protection statutes also prohibit false or misleading advertising. In Ontario, for example, the *Consumer Protection Act*, provides that "where the Registrar believes on reasonable and probable grounds that a seller or lender is making false, misleading or deceptive statements in any advertisement, circular, pamphlet or similar material, the Registrar may order the immediate cessation of the use

---

<sup>16</sup> *Bensusan Restaurant v. King*, 937 F. Supp. 295 (S.D.N.Y. 1996)

<sup>17</sup> R.S.C. 1985, chap. C-34, section 52

<sup>18</sup> Davies, Ward & Beck. *Competition Law of Canada*, Vol. 1 (New York: Juris Publishing, 1997) at § 6.02

<sup>19</sup> *Competition Act*, R.S.C. 1985, chap. C-34, section 52(2)(f) and (g)

of such material..."<sup>20</sup>. These provisions would apply to advertising or solicitations made over the Internet, although it is unclear whether the jurisdiction of the Ontario Registrar is limited to communications that originate within the province or would extend to any communication that is received in Ontario.

In response to concerns about junk e-mail and advertising directed at children over the Internet, the Canadian Direct Marketing Association is reported to be updating its compulsory code of ethics to include Internet advertising.<sup>21</sup> The Code of Ethics and Standards of Practice is a voluntary code, adopted by the Canadian Direct Marketing Association and its members. The Code includes, among other things, policies for the collection, use and distribution of personal information about individuals, in an effort to ensure that consumers' privacy rights are protected. Personal information is not to be included in lists made available for sale or rental, if there is a reasonable expectation on the part of the individual at the time the information was collected that it would be kept confidential. Members are required to delete names and other information from their lists when requested. The proposed changes to address electronic advertising will presumably deal with such issues as the collection of personal information for the purposes of targeted advertising over the Internet.

Your client has to be aware that, depending on the product that it sells, it may not be able to advertise the product on a worldwide basis. For example, if your client sells alcohol or certain reading material, it may not be able to advertise in some countries. There are different standards and advertising rules with respect to children's advertising in many countries and your client should investigate the requirements before it spends significant amounts of money on Internet advertising campaigns that must be changed.

Clients that sell medical products, pharmaceuticals, herbal products and certain safety products for example, must determine the regulatory requirements that they must adhere to. They may be quite different in the countries where your client expects to get "hits" on its site. Your client's liability for damage or injury caused by its products may also vary depending on the country in which the product was ultimately purchased.

The client also has to be aware that the rules governing comparative advertising are not the same in all countries and what is permissible in its home jurisdiction may result in serious legal liability in another country. If the client is running a contest or game, they must check to see whether it is even legal to do so.

If the client has a registered trademark that they use in Canada, it may not have the right to use that mark in any other country. They could face legal proceedings by advertising that trademark in another country where their web site is operating.

---

<sup>20</sup> *Consumer Protection Act*, R.S.O. 1990, c. C. 31, section 38.

<sup>21</sup> (1997) 2:2 *Cyberspace Lawyer* 29.

## Electronic Evidence

Will the electronic records prepared by your client in the course of operating the business be admissible as evidence?

Business records have long been admitted in evidence in Canadian courts, if the record was made by a person with personal knowledge of the matter recorded and a duty to make the record, on the basis that such records can be shown to be both necessary to the conduct of business and reliable, since the business relies on them for its normal operations.<sup>22</sup>

However, the "best evidence rule" required the production of an original document in order to prove its contents. This rule applies to any form of recorded writing, including information stored in a computer. The original document is considered "primary evidence." Copies of the original and other types of proof, admissible when primary evidence is unavailable, are considered "secondary evidence." In the early years of computerized business records, courts struggled to determine whether a printout of a computer record was an original or a copy.

Federal and provincial evidence statutes attempted to deal with this issue by permitting the admission of copies of original documents into evidence. However, it was often necessary to produce witnesses to give evidence of the authenticity and reliability of the business records and of the copies generated by the computerized record-keeping system.

The courts have held that there must be sufficient evidence to demonstrate that the computer records are reliable, credible and trustworthy.<sup>23</sup>

The standards for electronic evidence developed by the Canadian Information and Image Management Society<sup>24</sup> suggest a number of questions which may be asked when considering both the admissibility of computer records and the weight to be given to the evidence, including:

- How reliable are the original sources of the data on which the record is based?
- Was the data recorded contemporaneously with the events to which the data relate, or within a reasonable time afterward?

---

<sup>22</sup> *Ares v. Venner*, [1978] 1 S.C.R. 591.

<sup>23</sup> *R. v. Sheppard* (1992), 9 Nfld. & P.E.I.R. 144 (Nfld. S.C.).

<sup>24</sup> National Standard of Canada: Microfilm and Electronic Image as Documentary Evidence, CAN/CGSB - 72.11-93.

- Was the data regularly supplied to the computer system of the organization that produced the record and was the data recorded in the usual and ordinary course of business?
- Do the processes by which the data was recorded conform to standard industry practices?
- Do the processes by which the data is stored and processed ensure the integrity of the data maintained by the computer system?
- Do the procedures by which the printout of the record was made conform to standard industry practices?
- Does the party producing the record rely on the data for its own internal business purposes?
- Is the data confidential, privileged or protected by some other rule of law or evidence which prevents or limits its disclosure in the subject legal proceedings?

The existence of a formal description of the computer record keeping system, produced for the purpose of operating the system rather than for the purpose of litigation, will assist in establishing the reliability of the computer data. Separating the responsibility for entering, maintaining and reproducing records in order to prevent intended or unintended modification of the data will also help make the records more reliable.

### *Canada Evidence Act*

Section 30 of the *Canada Evidence Act* governs the admissibility of business records generally. A record made in the usual and ordinary course of business is admissible where oral evidence in respect of the matter would be admissible. A copy of a record is admissible if accompanied by a statement as to why the original cannot be produced and a statement that attests to the copy's authenticity. "Record" is defined as the whole or any part of any book, document, paper, card, tape or other thing on or in which information is written, recorded, stored or reproduced. Section 30 has been held to apply to computer records, in the same manner as paper records.

In *R. v. Bell*<sup>25</sup>, the Ontario Court of Appeal stated that the record may be in any form, and the form in which the information is recorded may change. A record may also be a compilation of other records, such as a bank statement that is compiled from records of individual transactions. The court also concluded that it is possible for a record to exist in more than one form at any given time. For example, the same information may be recorded in different forms for different purposes. All such records may be admissible under either section 29 or section 30 of the Act.

---

<sup>25</sup> (1982), 26 C.R. (3d) 336.

### Bill C-54

On October 1, 1998, Bill C-54 *The Personal Information Protection and Electronic Documents Act*, was given first reading. The stated purpose of the bill is to "support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the *Canada Evidence Act*, the *Statutory Instruments Act* and the *Statute Revision Act*".

In Part 3 of the bill, the *Canada Evidence Act* is proposed to be amended to add that any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.<sup>26</sup>

The bill also provides that the best evidence rule in respect of an electronic document is satisfied (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or (b) if an evidentiary presumption established under section 31.4 applies. An electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout. In the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven (a) by evidence that supports a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system; (b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or (c) if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it.<sup>27</sup>

### Intellectual Property Rights

What about copyright infringement and the use of your client's trademarks on the Internet?

---

<sup>26</sup> Bill C-54, Part 3, clause 56.

<sup>27</sup> Bill C-54, Part 3, clause 56.

### Copyright

As most lawyers know, copyright in Canada is created by the *Copyright Act*.<sup>28</sup> The exclusive rights of the copyright owner relevant to online communications include the right to produce or reproduce the work; publish the work; perform the work in public; communicate a work to the public by telecommunication; and authorize others to do any of the foregoing.

The author has the moral right to the integrity of the work and to be associated with the work or to remain anonymous. These moral rights are separate from the copyright. They may be waived, but cannot be assigned or transferred.<sup>29</sup> Electronic commerce can pose a threat to the integrity of copyrighted works as the public is now able to effortlessly transform or sample portions of works. These capabilities can also result in the disassociation of original copyrighted works from their authors.<sup>30</sup>

It is possible for an Internet user to violate several of the copyright owner's exclusive rights simultaneously.

E-mail messages, which form the vast majority of online communication, may infringe copyright in a number of ways. The sender of the message may infringe by including a reproduction of a copyright work in the message. The recipient may infringe by copying it and forwarding it to one or more other persons. Posting an e-mail message on a public mailing list or newsgroup may also be considered a communication to the public and infringe the copyright owner's exclusive right to communicate a work by telecommunication.<sup>31</sup>

The World Wide Web is also a common source of copyright infringement. Publishing a work on a Web page without the copyright owner's permission will constitute both an unauthorized reproduction of the work and a communication of the work to the public. If the work was previously unpublished, it would also constitute an unauthorized publication of the work.

Web pages are frequently copied — or cached — by Internet Service Providers (ISPs) and end-user browser programs to increase the speed at which the pages are accessed and to decrease network traffic. Caching is technically a reproduction of the

---

<sup>28</sup> R.S.C. 1985, c. C-42.

<sup>29</sup> *Copyright Act*, R.S.C. 1985, chap. C-42, as amended, section 14.1.

<sup>30</sup> See generally Racicot *et al.*, *Internet Content-Related Liability Study*, Industry Canada, 1997.

<sup>31</sup> "Copyright and the Information Highway," *Final Report of the IHAC Copyright Subcommittee*, (Ottawa: Industry Canada, 1995).

work and, therefore, an infringement unless it is authorized by the copyright owner, even if the caching is done unwittingly. Knowledge and intent are not relevant to infringement.<sup>32</sup> However, if a copyright owner makes material freely accessible on the Web, there is also an implied license to make ephemeral copies by browsing or caching, if such copies are necessary to access the information.<sup>33</sup>

Canadian law does not recognize copyright in a title.<sup>34</sup> The reproduction of another Web page's universal resource locator (URL) will not likely be viewed as an infringement of copyright. An URL is merely a descriptive pointer to the page address, and is analogous to a title.

### *Trademarks*

There are no special online trademark rights. However, one may acquire trademark rights through online use. The *Trademarks Act* provides that a trademark has been adopted in Canada when a person starts to use it in Canada or to make it known in Canada or, when that person files an application for registration in Canada.<sup>35</sup>

A trademark is used in association with goods if it is: (1) marked on the goods; (2) marked on the packages in which the goods are distributed; or (3) associated with the goods in a manner that gives notice to the purchaser of the goods at the time of change of title or possession. A trademark is used in association with services if it is displayed during the performance or advertising of the services. The use of a trademark to advertise goods does not constitute use under the *Trademarks Act*.<sup>36</sup> Accordingly trademark rights may be established by advertising services electronically, but trademark rights cannot be acquired online if the mark is associated only with goods that must be delivered physically.

A trademark is deemed to be made known in Canada when it has been used in association with wares or services by a person in a country of the Union for the Protection of Industrial Property, or of the World Trade Organization and wares are distributed in association with the mark in Canada; or the wares or services have been advertised with it in Canada in printed publications or radio broadcasts, so that it has become well known in Canada. Revisions of the *Trademarks Act* have been proposed,

---

<sup>32</sup> *Ibid.*

<sup>33</sup> *Supra*, note 31.

<sup>34</sup> *British Columbia v. Mihaljevic* (1989), 26 C.P.R. (3d) 184 at 190; affirmed (1991), 36 C.P.R. (3d) 445 (B.C.C.A.).

<sup>35</sup> *Trademarks Act*, R.S.C. 1985, chap. T-13, as amended, section 3.

<sup>36</sup> *Trademarks Act*, R.S.C. 1985, chap. T-13, section 4.

in which the restriction to advertising in printed publications or radio broadcasts would be removed, allowing any form of advertising to make a trademark well known in Canada.

The Internet can be viewed as a large advertising medium. Foreign trademark owners may therefore be able to acquire rights in Canada by advertising their wares or services on the Internet. Trademark owners from outside of Canada may also be able to acquire rights in Canada through the online distribution of wares coupled with the display of the trademark if such distribution causes the trademark to be well known in Canada.

### *Infringement*

The registration of a trademark under the Canadian *Trademarks Act* gives to the owner “the exclusive right to the use throughout Canada of the trademark in respect of those wares or services.”<sup>37</sup>

As noted above, the Act distinguishes between goods (wares) and services. Most electronic commerce transactions include the provision of services. Therefore, advertising those services online may constitute an infringement of Canadian trademark rights, even if the advertisement originates outside Canada.

To the extent that goods may be delivered electronically — for example, software may be downloaded from a Web site — Canadian trademark rights would be infringed if the mark is displayed on the goods or included in the transferred data. Contracts concluded completely electronically may also give rise to trademark infringement if the courts recognize transfer of title on the basis of the electronic contract, and there is display of the trademark in conjunction with the contract.<sup>38</sup>

The *Trademarks Act* also provides that the use of a confusingly similar trademark is an infringement of a registered trademark, and prohibits using a registered trademark in such a way as to cause depreciation of good will in that mark.<sup>39</sup> Anyone posting content on the Internet that contains another person’s trademark may be liable for direct infringement under sections 19, 20 and 22 of the Act. Others who act as facilitators or intermediaries for direct infringers, such as ISPs, may also be liable as vicarious or contributory infringers.

---

<sup>37</sup> *Trademarks Act* R.S.C. 1985, chap. T-13, section 19.

<sup>38</sup> *Supra*, note 31.

<sup>39</sup> *Trademarks Act*, R.S.C. 1985, chap. T-13, sections 20 and 22.



### *Internet Domain Names*

Internet addresses themselves may also pose trademark problems. Commonly called "domains", these addresses are made up of a trade name selected by the user, followed by one or more suffixes that identify the type or location of the organization. Names are issued on a first-come, first-served basis by non-profit groups that have taken on the task of keeping track of the computers linked to the Net.

The Canadian Domain Name Registry for the CA top level domain is administered by the CA Domain Committee and the University of British Columbia. To obtain a CA Domain registration, one must fill out and submit a detailed application template to the registry.

Because of the restrictions imposed on the allotment of the CA domain names, many corporations which do not qualify for top-level, pan-Canadian domain names opt instead for one of the international COM, EDU, NET, ORG, or GOV international domains allocated by InterNIC. Canadians who wish to obtain these functional domains are subject to the InterNIC rules. All registrants are required to certify that, to the best of their knowledge, the use of the domain name does not violate trademark or other statutes. The evolving policy of InterNIC has been to allow owners of registered trademarks to claim domain names that are the same as their trademark, even if someone else has been previously granted them. However InterNIC registers names worldwide, and InterNIC has been unable to resolve disputes between different owners of the same or similar trademarks in different countries.

There has been one reported "passing-off" case<sup>40</sup> where the plaintiff did not have a registered trademark and applied for an interlocutory injunction restraining the defendant from using the name "pei.net." The plaintiff was unsuccessful. It failed to establish all three elements of the passing off: (1) the existence of good will; (2) deception of the public due to a misrepresentation; and (3) actual or potential damage to the plaintiff. The court found that the plaintiff had not been "in business under its trade name for such a reasonable time and to such a reasonable extent that it [had] acquired a reputation under that trade name that would prevent the defendants from using a similar name." The plaintiff also failed to establish misrepresentation to the public. The allegedly infringing name was only in use a short time and the defendant stopped using it almost immediately after notice from the plaintiff. The plaintiff did not show any actual damages from the defendant's conduct, and due to the fact the defendant stopped using the domain name, there were no potential future damages.

This judgment demonstrates the difficulty the Canadian courts have in understanding the new information technology and in adapting existing law to it. For

---

<sup>40</sup> *PEINET Inc. v. O'Brien* (1995), 61 C.P.R. (3d) 334 (P.E.I. S.C.).

example, the trial judge drew a distinction between the defendant's lower-case domain name "pei.net" and the plaintiff's upper-case company name "PEINET Inc." This distinction is technically irrelevant with respect to domain names. Nevertheless, it seemed to provide the trial judge with a basis for differentiating the plaintiff's corporate name from the defendant's domain registration. The trial judge acknowledged the court's lack of technical expertise:

The case also illustrates the benefit of registering a domain name as a trademark. The plaintiff was obliged to meet a higher burden of proof to show passing off. Had the plaintiff owned a registered trademark in the domain name, it might have been able to show infringement through the use of a "confusingly similar" trademark contrary to section 20 of the *Trademarks Act*.

It should not come as any surprise that in many instances the link is a trademark associated with the other site. Does this constitute "use" of the trademark? If so, is an unauthorized hyperlink an infringing use? And, if it is infringing, where does the infringement occur — where the user's computer is physically located, where the trademark owner's computer is located, or in each jurisdiction where the Internet site may be accessed?

Your client should also be made aware that its use of its trademark as part of a domain name may infringe on another trademark for a completely unrelated product. Your client's registered trademark may be issued for use with stereos, but its use as part of a domain name that is transmitted everywhere, may infringe on another trademark registered in another country for the same or even different products.

## **Privacy**

What are your client's obligations with respect to personal or credit information that may be collected in the course of making sales over the Internet?

A client that intends to sell goods or services over the Internet will probably also be collecting personal and credit information about their customers. The customer might voluntarily enter the information, or the system may obtain some of the information through the use of "cookies". The client needs to be made aware of the need to maintain adequate security measures, not only to protect the client's own systems and information, but also to maintain the privacy of the personal information and credit details of its customers. The client should consider formulating and publishing a consumer privacy policy that will advise its customers of their rights with respect to their data held by the client. The client must then make sure that they take all necessary steps to maintain the policy. The computer security systems available as well as the advances in encryption and digital signature technology can all assist the client in keeping its confidentiality obligations.

The Government of Canada has formally adhered to the Organization for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the OECD Guidelines). The principles reflected in the OECD Guidelines have been adopted by agencies of the federal government. The OECD Guidelines are also reflected in privacy legislation passed by the governments of the various provinces and in voluntary codes adopted by a number of industry groups.

The federal *Privacy Act*<sup>41</sup> and *Access to Information Act*<sup>42</sup> govern the collection and use of personal information by governments and quasi-governmental agencies.

Quebec is the only province that has enacted privacy legislation governing the private sector.<sup>43</sup> Within the Quebec public sector, the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*<sup>44</sup> applies to approximately 3,600 public bodies, including municipal governments, schools, universities, health and social services. In Ontario, the equivalent statute is the *Freedom of Information and Protection of Privacy Act, 1987*.<sup>45</sup> Other provinces have adopted similar legislation.<sup>46</sup> While the laws of each jurisdiction vary in their details and procedural requirements, most are based on the OECD Guidelines.

Specific statutes in areas of federal jurisdiction (such as banking) or provincial jurisdiction (such as consumer credit reporting) regulate the collection and use of personal information in those industries.<sup>47</sup>

Administrative tribunals have adopted policies and regulations that have either a direct or indirect impact on privacy and electronic commerce. For example, the Canadian Radio-Television and Telecommunications Commission (CRTC), which

---

<sup>41</sup> R.S.C. 1985, chap. P-21.

<sup>42</sup> R.S.C. 1985, chap. A-1.

<sup>43</sup> *Act respecting the protection of personal information in the private sector*, S.Q. 1993, chap. 17.

<sup>44</sup> S.Q. 1982, chap. 30.

<sup>45</sup> R.S.O. 1990, chap. F.31.

<sup>46</sup> Manitoba: *Freedom of Information Act*; S.M. 1985-86, chap. F175; New Brunswick: *Right to Information Act*, S.N.B. 1978, chap. R-10.3, as amended; Newfoundland: *Freedom of Information Act*, S.N. 1981, chap. 5, as amended; Nova Scotia: *Freedom of Information Act*, S.N.S. 1990, chap. 11.

<sup>47</sup> See, for example *Bank Act*, S.C. 1991, chap. 46; *Consumer Reporting Act*, R.S.O. 1990, chap. C-33, R.S.N.S. 1989, chap. 93, R.S.P.E.I. 1988, chap. C-20; *Credit Reporting Act*, R.S.B.C. 1979, chap. 78; *The Personal Exemptions Act*, R.S.M. 1987, chap. P.34; *Consumer Reporting Agencies Act*, R.S.N. 1977, chap 18; *Credit Reporting Agencies Act*, R.S.S. 19, chap. C-44.

regulates telephone utilities has adopted regulations with respect to the use of automatic dialing devices.

Guidelines established by private bodies, such as the Canadian Bankers' Association and the Canadian Direct Marketing Association also have an impact on privacy in electronic commerce transactions. While the private guidelines do not carry any force of law, they are generally consistent with the OECD Guidelines and with federal and provincial privacy legislation. They are widely followed within the applicable industries, as an informal means of self-regulation. The Canadian Standards Association, in conjunction with business and consumer groups, recently developed a model privacy code that it urges be voluntarily adopted by the private sector.<sup>48</sup>

### *Consumer Reporting Legislation*

Provincial consumer reporting legislation governs the activities of private entities that collect and distribute credit and financial data of individuals.<sup>49</sup>

In Ontario, the *Consumer Reporting Act*<sup>50</sup> requires the registration of consumer reporting agencies, regulates the disclosure of data and the contents of credit reports, prohibits the disclosure of certain types of data, and creates rights for consumers to have access to, and to require correction of, data about themselves. The Act also establishes administrative procedures for enforcing the regulations and for investigating complaints with respect to consumer reporting agencies. The statutes in other provinces are generally similar.

Regulations under the *Ontario Collection Agencies Act*<sup>51</sup> prohibit collection agencies from disseminating false or misleading information that may be detrimental to a debtor or any member of his or her family, and provide remedies to individuals in

---

<sup>48</sup> Canadian Standards Association, Draft Model Code for the Protection of Personal Information, 1996.

<sup>49</sup> British Columbia: *Credit Reporting Act*, R.S.B.C. 1979, chap.78; Manitoba: *The Personal Investigations Act*, R.S.M. 1987, chap. P34; Ontario: *Business Practices Act*, R.S.O. 1990, chap. B.18; *Consumer Protection Act*, R.S.O. 1990, chap. C.31; *Consumer Reporting Act*, R.S.O. 1990, chap. C.33; Newfoundland: *Consumer Reporting Agencies Act*, R.S.N. 1977, chap. 18; Nova Scotia: *Consumer Reporting Act*, R.S.N.S. 1989, chap. 93; Ontario: *Business Practices Act*, R.S.O. 1990, chap. B.18; *Consumer Protection Act*, R.S.O. 1990, chap. C.31; *Consumer Reporting Act*, R.S.O. 1990, chap. C.33; Prince Edward Island: *Consumer Reporting Act*, R.S.P.E.I. 1988, chap. C-20; Saskatchewan: *Credit Reporting Agencies Act*, R.S.S. 1978, chap. C-44; Alberta: *Consumer Credit Transactions Act*, S.A. 1985, chap. C-22.5.

<sup>50</sup> R.S.O. 1990, chap. C.33.

<sup>51</sup> R.S.O. 1990, chap. C-14.

situations where false or misleading information is disseminated. With the exception of Manitoba and Quebec, each province has debt collection agency legislation with provisions similar to those in Ontario.

Bill C-54, mentioned previously, attempts, in Part 1, to protect the privacy of personal information collected in the course of commercial activities or disclosed or used interprovincially or internationally. The Bill will make interesting reading as it progresses through subsequent readings in the House of Commons to see what final requirements are imposed on private organizations to protect the privacy of personal information they collect in the course of operating in an electronic environment.

### **Dispute Resolution and Arbitration**

How will contract and product performance disputes be resolved? What if your client is in Winnipeg and the customer purchased products from the web site while living in California?

For hundreds of years, commercial entities and individuals have pursued their contractual remedies and resolved their problems by resorting to the court systems available in their jurisdictions. This will continue.

As the electronic business community increases in its size, influence and demands, however, it is finding more dissatisfaction with the traditional, adversarial court system and is looking for alternative ways to solve disputes and resolve issues. Alternative Dispute Resolution (ADR) does not, for the most part, involve the endless motions, voluminous proceedings, procedural wrangling and years of arguing and waiting for a judgment that characterize the "old" litigation system for most modern business people and consumers.

Many governments are considering requiring contracting partners to submit their disputes to some form of ADR prior to, or instead of being permitted, to access the courts.

#### *ADR for Electronic Commerce*

ADR presents an attractive alternative for many businesses involved in electronic commerce transactions since it is possible to have the dispute resolved by a technical expert in the area instead of a judge or a lawyer and, if the system works as it should, it can take much less time to reach a decision or a settlement.

Cost is also a factor, since businesses that are used to the savings they perceive to be available through electronic commerce do not want to waste the management time and money usually required to take a dispute through the usual trial process.

Confidentiality is also a factor and the thought that the details of an ADR proceeding are not going to be splashed over the front page of the local and financial press is attractive. This is particularly important when the dispute arises out of a failure of security systems to function, or as a result of a technical problem with a major system. Most companies do not want this to be in the next issue of reported cases.

A couple of pilot ADR projects are being started around the world to resolve on-line disputes and many organizations are working on model laws to deal with uniquely electronic issues.

Unique issues and problems can arise in electronic commerce, particularly involving consumers.

### *Types of Disputes*

The usual "net" disputes exist and can be expected to continue, including problems over postings on the Internet; the use of trademarks belonging to third parties; issues with domain names; and infringement.

There will undoubtedly also be issues that are more usually encountered in our "traditional" modes of commerce such as disputes over the quality of goods purchased on-line; failures to deliver; and errors in order taking and failures to pay.

Although traditionally this latter group of disputes has occurred between trading partners who, even if they do not do business face to face, at least probably know where the other party carries on business, it is just as likely that a party may not even know what continent the other party is really on, let alone be able to get hold of that party to serve them with a writ or enforce a judgment.

Some experts involved in the IT industry have opined that electronic commerce will not fulfill its true potential globally unless the participants to a transaction can be assured of remedies and enforcement vehicles to redress purely commercial grievances in a manner that does not require them to appear in a courtroom half-way around the world.

One solution is the development of a form of on-line commercial dispute resolution mechanism that would allow for speedy adjudication of commercial complaints arising from on-line transactions. In the United States, The Virtual Magistrate Project is in the pilot stage. It deals with Internet related disputes, but its focus is mainly on complaints

about postings; messages, infringement, defamation, inappropriate materials or other content issues.

Although this is a valuable and necessary undertaking, the Virtual Magistrate Project, in its present form, is not meant to handle "supply and payment" issues. How will a buyer get redress if it receives faulty materials in an on-line order and the supplier is located half a world away?

### *Alternative Methods of Dispute Resolution*

Mediation is flexible and informal and involves the parties' agreement to submit to mediation. The parties may use pre-defined rules or set their own. The process has the advantage of allowing the parties to use a mediator with particular technical expertise. The parties can deal with the issues with the mediator, keeping the conflict level down and increasing the likelihood of keeping a healthy business relationship.

The success of mediation of course depends to a large extent on the skill and knowledge of the mediator and his or her skill at negotiation. The mediator must guide the parties to a solution, not impose it, and must not take over the process. Mediation may not be effective if the parties are acrimonious and are not willing to work together.

*Private court* is available in some jurisdictions and the numbers are increasing. Again, there is a written agreement between the parties to use the private court system. The private court has rules of procedure and also relies on provisions of various arbitration statutes. The adjudicators are usually lawyers or retired judges but do not need to be. The powers of the adjudicator may be similar to judicial powers, depending on the jurisdiction. In Canada, the parties can transfer disputes from the "public" court system to private court. The private court system usually involves a settlement conference similar to a pretrial, after which the adjudicator prepares a report on the status of the dispute and the settlement possibilities. The adjudicator has an active role and may also arrange for a procedural conference to deal with discovery and other issues.

The advantage of the private court system is that it is faster than the usual court system, as well as being flexible. There is a relatively speedy resolution to the dispute, with an emphasis on negotiation. The system is however, still adversarial and the skill level of the adjudicator may not be what is needed.

*Commercial arbitration* is available in most countries and the parties can agree that it is required for the resolution of certain specific disputes or all disputes arising out of the agreement. Various rules can be chosen to govern the procedure of the arbitrators in an international dispute, including the International Chamber of Commerce (ICC)

rules, the American Arbitration Association (AAA) International Arbitration Rules and the J.A.M.S./Endispute Arbitration Rules and Procedures.

The Convention on the Recognition and Enforcement of Foreign Arbitral Awards (“New York Convention”), signed in New York, on June 10, 1958, is an international treaty for the recognition and enforcement of arbitral awards made in one state other than the state where recognition is sought. It has always been a problem in an international setting to gain recognition and enforcement of the arbitration clause and then to enforce an award in a foreign jurisdiction. Since 1958, 108 countries have become parties to the New York Convention.

### *New Initiatives*

#### i. The Virtual Magistrate Project (United States)

This project was set up to resolve disputes on worldwide networks about on-line messages, postings, infringement, misappropriation of trade secrets, defamation, deceptive trade practices, inappropriate materials on the Internet and invasion of privacy disputes. The parties are the users of the Internet, those harmed by wrongful messages postings or files and system operators (sysop’s).

The goal is to establish the feasibility of on-line dispute resolution for disputes that originate on-line. It provides for rapid, low cost and accessible remedies and operates with either a single magistrate or a panel of three arbitrators selected by the American Arbitration Association and committee of Cyberlaw Institute Fellows.

Filings to the Virtual Magistrate are done by email. The arbitrators will not automatically apply the law of a particular jurisdiction, but will look at what is appropriate. Decisions are supposed to be rendered within 72 hours after all parties participate. The decisions usually involve deciding whether to mask, delete or restrict access to a message, file or posting; whether to disclose the identity of an individual; or whether to deny access to the on-line system.

The sysop’s are expected to support and enforce decisions of the arbitrators and third parties will be asked to comply with the decision in return for the use of the Virtual Magistrate process. Both users and sysops waive all claims against the arbitrators.

One of the problems with the Virtual Magistrate system may be its concentration on U.S. law and U.S. issues. Electronic commerce will only be truly valuable when it is global and U.S. law is too narrow — one party may be in the U.K. and one in Africa.



- ii. Is it time for an on-line international arbitration mechanism — the World Wide Court (WWC)?

In the WWC, the adjudicators and mediators would be on-line and would include representatives from many countries. The adjudicators would handle commercial disputes from businesses and consumers and, like the Virtual Magistrate project, complaints and "pleadings" would be handled on-line.

It would not matter where in the world the parties were. The adjudicators would apply whatever local law was reasonable in the circumstances. The adjudicators could be lawyers but it would be preferable to have a significant involvement from the business and technical communities.

Legal issues with respect to evidence, contract formation and acceptance as well as other "contract" issues, where appropriate, could be settled by reference to the UNCITRAL Model Law on Electronic Commerce. The decisions would be rendered promptly on-line and could, at the simplest level, involve requiring a supplier to provide a replacement product. In many cases, the amounts involved may not be large, but in order to have large volumes of transactions that electronic suppliers dream of, there will have to be a mechanism to handle all types of problems.

Perhaps a condition of access to the Internet for a company and its customers would be the consent of both parties to submit disputes to the WWC for resolution. This might solve the jurisdiction problem. The agreement to submit to the WWC could be done by way of a click and consent agreement posted on the supplier's site.

Once the system is well known and accepted, suppliers would have to post a warning notice if they were not part of the WWC. Perhaps the WWC could institute a certification system that suppliers would post (like the Good Housekeeping seal). This would advise consumers and contracting partners that the supplier was a member of the WWC and therefore willing to submit any disputes to adjudication by the on-line mediator or arbitrator. It might assist in instilling confidence in on-line contracts if the supplier agreed to be subject to a third party procedure to resolve problems.

Consumers and other parties could be asked to post a reasonable bond to cover the cost of the adjudication — perhaps by credit card.

This process could make it easier for consumers to accept making their purchases over the Internet — since they would not have to sue the supplier in a foreign jurisdiction and could choose not to deal with suppliers that did not belong to the WWC. If a supplier refused to comply with an order of the WWC, their certification would be revoked until they agreed to do so.

If confidence is enhanced in the Internet buying process, then sales should increase and suppliers could expect to begin to increase their profits and decrease the uncertainties of operating in this “virtual” global market.

Just a thought.

## **Conclusion**

The last couple of years in Canada have seen a growing awareness by many diverse groups of the changes that need to be made to Canadian law and policy in order to have Canadian commerce and the rules governing the conduct of commerce remain current with the advances in technology. This is needed, not only to protect the creators of works used in an electronic marketplace, but also to protect the consumers of goods purchased electronically and to ensure that businesses operating in that medium are sure of the rules and responsibilities governing their activities. These businesses must also be assured that their “electronic” contracts can be enforced.

Courts in Canada and other common law countries have shown themselves to be very flexible in adapting contract law principles to new technologies and business practices. Courts are willing to look past the formal requirements of writing and manual autograph signatures. They are more concerned with policies behind those requirements — ensuring the reliability and authenticity of legal agreements.

The pace of change in the law of electronic commerce is such that any description of the law must quickly become incomplete. Some day, perhaps, there will actually be settled law in this dynamic area. In the meantime, those involved in electronic commerce must maintain an active watch on all new developments.

Commercial lawyers need to quickly become “Net-literate” and understand how the traditional legal environment — and their clients’ expectations — are changing.

It will not be easy. It certainly will not be boring either.