SOLVING LEGAL ISSUES IN ELECTRONIC COMMERCE

*John D. Gregory**

CONTENTS

* General Counsel, Policy Branch, Ministry of the Attorney General (Ontario). The author is indebted to Professor Amelia H. Boss for her helpful comments on a draft of this article.

This field is replete with acronyms. The principal acronyms in this article are:

ABA	American Bar Association
EU	European Union
NCCUSL	National Conference of Commissioners on Uniform State Laws (U.S.)
OECD	Organization for Economic Cooperation and Development
PKI	Public Key Infrastructure
SET	Secure Electronic Transactions protocol
UCC	Uniform Commercial Code (U.S.)
UECA	Uniform Electronic Commerce Act (Canada)
UETA	Uniform Electronic Transactions Act (U.S.)
ULCC	Uniform Law Conference of Canada
UNCITRAL	United Nations Commission on International Trade Law

I. INTRODUCTION

Electronic commerce is inspired by high technology, driven by competitive markets, and . . . impeded by old law. That is the perception held by many people, including a considerable number of lawyers. Yet electronic transactions account for billions of dollars each year, with astronomical growth rates in the recent past held out as promises for like or greater growth in the future. To what extent are these transactions unsupported by law, and how can the law catch up to where commerce needs it to be?

This article examines three types of intersection between law and electronic commerce: areas of uncertainty, statutory barriers, and measures of promotion. The first type involves mainly private sector activity to underpin e-commerce. The second involves private and public sector activity, as legislatures intervene to clear the path. The third involves mainly public sector actions, though private initiatives are found here too.

The thesis, to the extent that there is a thesis, is that the legal analysis of electronic commerce has undergone a process of simplification, for a number of reasons. The more one looks at the legal issues, the less awesome most of them appear, and the less radical the measures needed to ensure that the law does not unnecessarily impede e-commerce. The issues do not go away entirely, of course. Hard questions remain. Legislation needs to be passed.

But a total rethinking of what we know as commercial law seems increasingly unlikely.[1]

II. AREAS OF UNCERTAINTY

Electronic commerce rests largely on the law of contract, though of course other fields of law are relevant to some issues, such as intellectual property, civil procedure and evidence, not to mention criminal law.

1. Contract Questions

Ordinary contract questions — what is an offer, what is acceptance — did not slow people down much in doing electronic commerce bilaterally. Some harder questions arose about communications: when was the offer or the acceptance delivered? Who is responsible for miscommunication, especially when buyer and seller use intermediaries to handle their communications links? Over time it became clear that many of these issues had persuasive parallels in the paper world, and the assignment of responsibility on paper worked well for e-commerce too.

To some extent the questions arose not because of problems in the law but because commercial practices needed to settle down once they went electronic. For example, there has been some uncertainty about whether the owner of a World Wide Web site is making an offer or merely an invitation to treat. Does the potential customer's communication constitute an acceptance or an offer? The answer will influence the time and place the contract is made. But these are matters of intention. It is open to the web site owner to spell out the status of the content of the web pages. The difficulty in this example is more in knowing what to want than in knowing how to get what one wants. Negotiating with a web site presents other kinds of difficulties, but non-negotiable contracts are often enforceable, so some parties are able to give effect to their intentions.

1. The appearance of a number of new books on electronic commerce suggests that the topic is more approachable than formerly: see, for example, George Takach, *Computer Law* (Toronto, Irwin Law, 1998); A. Gahtan, M. Kratz and F. Mann, *Internet Law: A Practical Guide for Business and Professionals* (Toronto, Carswell, 1998); and the monumental work by Pierre Trudel *et al.*, *Le Droit du cyberespace* (Montréal, Thémis, 1998).

In some cases, the courts will work out the new legal rules if one wants to wait for them to get there. For example, the common law provides that the acceptance of an offer is made when it is put in a mailbox addressed to the offeror (assuming that postal communication is acceptable). What of an electronic acceptance? Should it be considered made when the acceptor pushes the "send" button, or only when it is received?[2] What difference does the presence of intermediaries make, when they are arm's length service providers and not obviously agents of one party or the other?

2. Electronic Devices

Another hot topic is the status of electronic devices, sometimes called "electronic agents", that can be programmed to seek out information and to communicate what appear to be offers and acceptances without human intervention or review at the time of communication. May one make an offer or acceptance by machine? Is it possible to program enough artificial intelligence to make a machine a legal actor in its own right? Who may be responsible if the machine "makes a deal" contrary to the programmer's intention?

The debates on this topic in the early 1990s at the UNCITRAL[3] wrestled with whether computers could contract, as if they might have a legal personality of their own.[4] UNCITRAL ultimately took such machines to be instruments of the owner for the purposes of forming contracts, as can be seen in the Model Law on Electronic Commerce.[5] But the common law is still unclear on the legal effect of using the machine, even though the policy of owner responsibility seems generally accepted.

---

2. In *Bickmore v. Bickmore* (1996), 7 C.P.C. (4th) 294 (Ont. Ct. (Gen. Div.)), the court held that a faxed acceptance of a faxed offer was delivered when the acceptance was sent. Compare the English courts on telex messages, generally held to be received only on actual receipt: *Entores Ltd. v. Miles Far East Corporation*, [1955] 2 Q.B. 327 (C.A.) and *Brinkibon Ltd. v. Stahag Stahl und Stahlwarenhandelsgesellschaft m.b.H.*, [1983] 2 A.C. 34 (H.L.). The latter decision contains useful consideration of the nature of instantaneous communications, concluding that no universal rule can cover all such cases.
3. United Nations Commission on International Trade Law.
4. See United Nations document A/CN.9/360, February 1992, para. 83-85. See also L. Wein, "The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence" (1996), 6 Harv. J. Law & Techn. 103; L. Solum, "Legal Personhood for Artificial Intelligences" (1996), 70 N.C. L. Rev. 1231.
5. United Nations Model Law on Electronic Commerce, 1996. See http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm.

It is arguable that legislatures should intervene on such questions and spell out the answers so business does not have to wait on court decisions that could take years to form a consistent and authoritative message. As a result, one sees the United Nations Model Law answering these questions, as does the draft Uniform Electronic Transactions Act in the United States.[6] The work on the Canadian Uniform Electronic Commerce Act has only recently progressed to the law of electronic contracting.[7]

Meanwhile, or instead, many businesses dealing electronically have created their own legal framework, answering many of these questions by particular contracts known as "trading partner agreements".[8] Most trading partner agreements provide, for example, that an acceptance is received only when it comes into a computer system under the control of the offeror, and not when it is sent into cyberspace by the offeree. Most contain procedures for verification of communications, and the keeping of logs so disputes can be avoided or resolved. Over time, a number of questions without definite answers in the general law have taken on accepted answers through private lawmaking. Standard forms of trading partner agreements, even on the international level, have harmonized legal expectations to a large extent.[9]

The nature of electronic commerce is changing, however, and bilateral agreements are harder to arrange when one is dealing with strangers over an open system like the Internet. Open system commerce poses many of the problems of uncertainty in today's law. The less opportunity there is for private contractual solutions, the greater the demand one feels for legislation.

---

6. The Uniform Electronic Transactions Act (UETA) is being prepared by the National Conference of Commissioners on Uniform State Laws (NCCUSL). See http://www.law.upenn.edu/library/ulc/ulc.htm#ueccta for drafts.
7. The Uniform Electronic Commerce Act (UECA) is being prepared by the Uniform Law Conference of Canada. See http://www.law.ualberta.ca/alri/ulc/eindex.htm under "Electronic Commerce". In particular see Ian Kerr, "Providing for Autonomous Electronic Devices in the Uniform Electronic Commerce Act" at that site.
8. See Electronic Data Interchange Council of Canada, *Model Form of Electronic Data Interchange Trading Partner Agreement and Commentary* (Toronto, EDI Council of Canada, 1990) and Amelia H. Boss and Jeffrey B. Ritter, *Electronic Data Interchange Agreements: A Guide and Sourcebook* (Paris, International Chamber of Commerce, 1993).
9. Amelia H. Boss, "Electronic Data Interchange Agreements: Private Contracting Towards a Global Environment" (1992), 13 Nw. J. Int'l L. & Bus. 31. Much of the U.N. Model Law was influenced by the content of these private agreements.

Several other areas of uncertainty have not yet attracted statutory fixes, and it is arguable that the level of uncertainty associated with them is nevertheless decreasing. They are shrinkwrap licences and their electronic counterparts, "webwrap" and "clickwrap" licences; negotiable instruments; electronic money; the determination of jurisdiction, particularly civil jurisdiction, over electronic activities; and intellectual property questions. The latter two are the subject of separate articles in this symposium, so the description here will be brief.

3. Shrinkwrap Licences

A shrinkwrap licence is most often a licence whose terms are contained in or on a box containing computer software which is sealed with shrinkwrap plastic. The licence says that by removing the shrinkwrap, the buyer accepts the terms of the licence. Producers of software say they need this kind of immediately effective licence to ensure that the buyer is bound before he or she has a chance to copy the software or pass it on to others. That way they will have a legal remedy if they can detect the breach of the licence. Waiting for the buyer to use the software, or even to read the terms after opening the package, will not work, it is alleged, because the buyer can do harm to the producer before using the software or reading the terms.[10]

The shrinkwrap licence is an extreme example of the standard form contract that has been around in our law for many years. That the buyer has no chance to negotiate the terms is not fatal to the validity of the contract. That the buyer may choose not to read the terms is also not fatal. That the buyer does not even have the chance to read them if desired presents difficulties. In contract law this is obviously problematic. The terms of the licence are part of the contract, and the buyer must agree to the terms of the contract before he or she can be bound to them. How can the buyer even know that he or she is making a licence, not buying goods? If the terms cannot be known until the contract is in effect, how can they be incorporated into it? The contract must have been made in all its essential elements before the terms came to the buyer's attention, so those terms are not part of the deal.

10. See the policy discussion in the commentary to then proposed Article 2B of the Uniform Commercial Code in the United States: http://www.law.upenn.edu/library/ulc/ucc2b/2b898.htm, Preface (August 1998 draft).

Only one reported case in Canada has considered a shrinkwrap contract and there the court held it to be unenforceable.[11] In the United States surprisingly few cases have focused exclusively on the basic question of enforceability, rather than on collateral questions such as the relation between copyright law and contracts. The leading case holding such contracts valid depended on a number of factors beyond the form of the basic licence, including the presence of a clickwrap licence in the software that the defendant had activated.[12]

However, that case did find some facts that may be useful to those who wish to establish shrinkwrap licences. The package stated readably that it contained a licence whose terms would bind the buyer on opening. The buyer had an opportunity to return the contents unused at the expense of the producer if he or she did not like the terms once read. As a result, it is arguable that the full contract did not take effect until after opening, when the buyer decided to return or keep the product. In the alternative, if the contract was made at the time of payment for and delivery of the package, giving a right of rescission makes the imposition of extra terms less offensive or unfair.

It is at least arguable that properly designed shrinkwrap contracts can be valid in Canadian law if the principal terms ("This is a licence. You may not transfer or copy this software.") are readable from outside the package, and the subsidiary terms give the right of rescission to an unhappy buyer. However, those facts have not yet been before a court.

In the United States an effort is being made to draft uniform legislation specifically to deal with information licensing, and especially software licensing.[13] The draft provisions of the Uniform Computer Information Transactions Act, formerly draft Article 2B of the Uniform Commercial Code, make shrinkwrap licences enforceable, subject to the right of the buyer to return the software if

11. *North American Systemshops Ltd v. King* (1989), 68 Alta. L.R. (2d) 145, 97 A.R. 46 (Q.B.) The court acknowledged that different practices about notice of conditions might have changed the result.
12. *ProCD, Inc v. Zeidenberg*, 86 F.3d. 1447 (7th Cir. 1996). The case also turned to some extent on the reluctance of a federal court to apply state law to make the contract unenforceable. See also *Hill v. Gateway 2000*, 105 F.3d 1147 (7th Circuit 1997).
13. What was draft Article 2B of the Uniform Commercial Code became in April, 1999 a non-code statute. See http://www.nccusl.org/pressrel/2brel.html. For discussion of this controversial article, see *infra*, Section IV(2). More detail may be found at http://www.2bguide.com.

the terms of the licence are unacceptable. The debate continues. Little Canadian legislation is likely while the question is open in the United States.

4. Webwrap and Clickwrap Licences

"Webwrap" and "clickwrap" licences owe their name to the shrinkwrap licence, but they are quite different in operation. There is no "wrapping" involved.[14] A webwrap contract is one found on a web site. The visitor who wants to form a legal relationship with the site owner finds legal terms on the computer screen, often in a "dialogue box" that permits messages and responses. The visitor has to indicate consent to the terms, possibly by clicking a box on the screen that says "OK" or "I agree". A clickwrap contract works the same way, but it is installed in the medium, such as a diskette, which carries software. Before the program will install or operate the software, the user is led through the legal terms of the licence and has to indicate acceptance before the software will work.

Webwrap licences are less problematic than shrinkwrap licences because the user/licensee sees the terms before the contract is formed, or at least has an opportunity to review them if he or she wishes. Clickwrap licences may present themselves only after the software is paid for and delivered, so some mechanism may be necessary to ensure that the buyer can get the money back if the licence is not acceptable. Parties may face an evidence problem, especially for webwrap contracts: what were the terms to which the user agreed? Are the terms I click on today the same ones that will be there in six months, or at trial if there is a dispute? How does the buyer or user keep a record of what is in the dialogue box?[15] Some licences purport to bind the user to any changes that the producer chooses to make to the terms over the life of the licence, which for much consumer software is indefinite.[16]

14. Clickwrap licences are also known as point-and-click licences or click-through licences.
15. Sometimes technology can offer a solution. At least one vendor has software that will digitally sign the contents of the web page as read by the consumer, and again as signed by the consumer, so the integrity of the contents as read and signed can be demonstrated later. Other solutions provide for trusted third party storage of the secure contents of an electronic document.
16. A. Gahtan *et al.*, *Internet Law, supra*, footnote 1, p. 236.

Most of these challenges can be met by design and disclosure and do not appear to need legislative fixes in the near future.[17] If the courts resist enforcement of licences that appear fair to most observers, then that question may need to be revisited. This article will deal briefly with special concerns for consumer transactions further on.[18]

5. Negotiable Instruments

A negotiable instrument or negotiable document of title carries value; transferring the instrument transfers the source of the value, whether an order to a bank to pay money or title to goods in a warehouse or on a ship. For this reason the instrument must be unique. Only one claim may be made to represent a particular source of value. Electronic records are, however, infinitely reproducible. It does not yet seem possible to create a unique electronic record.[19] As a result, business people have had to find alternatives to negotiability. This task may be rendered more palatable by other commercial developments that have made negotiability less critical than it was when commerce was carried out in a world of strangers.[20] It is easier now to find trusted intermediaries for transferring value among strangers.

Some technological substitutes have been proposed. For example, the Comité maritime international (CMI) has developed a scheme by which title to goods on board a ship at sea may be transferred by a trustworthy electronic message to the ship, which then changes the registry on the spot. That way one need not have possession of a bill of lading to effect this transfer.[21] A similar regime has been approved for cotton warehouse holdings in the United States.[22] If one can deal authoritatively with proof of title

17. See Baker and McKenzie, "The Enforceability of Webwrap Licences", prepared for the Uniform Law Conference of Canada, 1998, at http://www.law.ualberta.ca/alri/ulc/eindex.htm under Electronic Commerce.
18. See *infra*, Section IV(3).
19. It may be possible to identify an electronic document by digital signature and time stamp and immobilize it in the hands of a depository, but that prevents its negotiability in fact.
20. See Jane K. Winn, "Couriers Without Luggage: Negotiability and Digital Signatures" (1998), 49 S. Carol. L. Rev. 739. See also J.S. Rogers, "The Myth of Negotiability" (1990), 31 B.C. L. Rev. 265.
21. *CMI Rules for Electronic Bills of Lading* (Paris, Comité maritime international, 1990). Further details are promised at http://www.bolero.com.
22. United States Warehouse Act, 7 U.S.C. Ch. 10, s. 259.

without dealing with the goods they represent, then one has less need to transfer the document of title. These examples bear on documents of title. Electronic cheques are still not possible. But the Depository Bills and Notes Act[23] goes some distance to establishing a commercially tradable market in electronic evidence of debt.

Technology evolves, of course. If a method is devised to create a unique electronic document, then we will see tension between whether the technology fits existing law or whether the law will have to change to meet new technology.[24] In the United States, Article 9 of the Uniform Commercial Code (the equivalent and originally the source of Canadian Personal Property Security legislation) has been changed to refer to "control" of "electronic chattel paper", to supplement the notion of possession of paper documents of title for creating and perfecting security interests and for establishing priorities.[25]

In short, private or statutory means may overcome the problems of electronic negotiability, not by recreating the same phenomenon but by permitting the same results through other paths.

6. Electronic Payment Systems

The difficulty of creating an electronic cheque has not brought electronic commerce to a halt or necessitated a wholesale downloading of parts of transactions onto paper at critical stages. Businesses have arranged other ways of transferring value, and banks have worked out a complex and effective worldwide method of handling funds electronically.[26] At the retail level, credit card and debit card transactions are carried out electronically every day. All of these arrangements rest on contract, not on statute (except for some consumer protection legislation).

Will the arrival of so-called electronic money make any difference? Apparently not in the short run.[27] E-money comes in two

23. S.C. 1998, c. 13.
24. See the symposium on electronic negotiability: (1995), 31 U. Idaho L. Rev. The American Bar Association is also considering the issues. See http://www.abanet.org/scitech/ec/ecp/electneg.html, which also lists sources. The draft UETA deals with "transferable records"; its coverage of documents otherwise covered by UCC rules is carefully refined.
25. Article 9 texts can be found at http://www.law.upenn.edu/library/ulc/ulc.htm.
26. See generally B. Geva, *The Law of Electronic Funds Transfers* (New York, Matthew Bender, 1992).
27. See Bradley Crawford, "Is Electronic Money Really Money?" (1997), 12 B.F.L.R. 399 (also at http://www.mccarthy.ca).

basic forms, access cards and stored-value cards.[28] Access cards are not much different from debit cards, except that a fixed store of value has been set aside for the card, which is used to access it. Stored value cards download the value onto the computer chip on the card, from which it is drawn without reference back to the source of the value. The latter model is used by Mondex, which is the subject of an extensive pilot project in the city of Guelph, Ontario.[29] No legislation has been enacted to support Mondex or stored-value cards generally, yet the pilot project goes forward. Once again, the network of contracts seems to be sufficient.

It may be that when commercial practices are more thoroughly developed, the need for some kind of supplemental or facilitating legislation will become apparent. But it will be important where legislation is passed that it not interfere with the ability of businesses and consumers to create their own effective systems. The credit card issuers are collaborating on what they call the Secure Electronic Transactions (SET) protocol for international electronic commerce.[30] It relies on a system of digital signatures and certificates issued by participants in the credit card network. However, the recent German statute on digital signatures may turn out to prohibit the deployment of SET in Germany for technical reasons relating to the medium of the signing key and the status of the certification authority.[31] Law reformers have to be sensitive to private initiatives, and the private sector to law reform proposals, to avoid unnecessary incompatibilities such as this.

Governments pay and are paid electronically too. The proposed Uniform Electronic Commerce Act, of which more will be said further on,[32] specifically authorizes governments to pay and be paid by electronic means. The Personal Information Protection and

28. Shameela Chinoy, "Electronic Money in Electronic Purses and Wallets" (1997), 12 B.F.L.R. 15.
29. See http://www.mondex.com.
30. See http://www.setco.org, http://www.visa.com/nt/ecomm/faq.htm#set and www.mastercard.com/set/.
31. An English text of the German statute is at http://www.kuner.com/data/sig/digsig4.htm. Whether this statute will in fact hamper such private systems as SET is a matter of some debate: see, for example, Stewart Baker, "International Developments Affecting Digital Signatures" (1997) at http://www.steptoe.com/WebDoc.NSF/Law+&+The+Net+All/International+Developments+Affecting+Digital+Signatures.
32. See http://www.law.ualberta.ca/alri/ulc/eindex.htm under "Current Civil Matters". For a discussion, see *infra*, Section III(4)(E)(i).

Electronic Documents Act, Bill C-54,[33] of which more will be said too,[34] authorizes incoming payments to the federal government to be made "in electronic form in any manner specified by the Receiver General of Canada".[35] It is admittedly easier to accept money than to pay it out; the debt to the government is not satisfied until the money is received, so the risk of an imperfect payment mechanism rests on the debtor. Opening the Consolidated Revenue Fund to withdrawals on electronic authorization is more risky. But again, it is not clear that a change in the law is needed to enable this, except perhaps for clarifying the authority where present authority seems too restrictive. For the rest, the technology will rule.

7. Jurisdiction

Until recently, most electronic commerce was done by electronic data interchange or otherwise on closed networks, *i.e.*, among parties bound to each other by contract or by adherence to a common system. It also involved trade in hard goods, tangibles, though the ordering and invoicing might well have been done electronically. Both these features meant that parties knew where the other parties were. The jurisdiction could be specified when the parties were identified, and goods had to be delivered to a real place. Much electronic commerce is still done in these conditions and therefore jurisdiction issues seldom arise.

Two developments aggravate jurisdictional problems. The first is the use of the Internet for trading, *i.e.*, over an open system where parties may have no previous (or future) relationship with each other. This can apply for business-to-business trade or for consumer purchasing. Consumer commerce has come into its own thanks to the graphic capacity of the World Wide Web. It is difficult or impossible to tell where a web site is "located", or more accurately, where the legally responsible person is located. This creates problems for civil jurisdiction (Where was the contract formed? Whose law applies?[36]) and also for enforcement of local laws against entities "present" in the territory only through a web site. As

33. See http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_2.C-54_cover-E.html.
34. See discussion *infra*, Section III(4)(E)(ii).
35. Section 34.
36. The place of contracting does not necessarily create jurisdiction for a court. See the Uniform Court Jurisdiction and Proceedings Transfer Act, http://www.law.ualberta.ca/alri/ ulc/acts/ejurisd.htm, section 10, commentary 10.2.

the technology permits "pull" relationships (I read or download what I go looking for on the web) and "push" relationships (the product vendor sends information to my computer automatically — sometimes but not always pursuant to my original request), the question of presence in a territory becomes more complex.

The second development is the growing commerce in intangibles, such as software, entertainment programs and other variants of intellectual property. Computerization and electronic communications have created markets and products that did not even exist a few years ago.[37] These intangibles can be delivered by the same electronic means used to order them. That gives the customer the same invisibility, or ubiquity, as the merchant. Either merchant or customer can hide behind an unlocatable "flybynight.com". So knowing the place for enforcement of the contract is even more difficult.

As George Takach has described in detail,[38] a number of cases in the United States have examined some of the ways that traditional jurisdictional rules have been applied to Internet transactions. A Canadian study was recently published by the Uniform Law Conference of Canada.[39] That study recommended a wait-and-see approach. Canadian courts have not yet "got it wrong".[40] In addition, the usefulness of a harmonized legislative approach across many borders is obvious, but developing such an approach will take time and hard thinking.[41]

Meanwhile, a good deal of electronic business is still done locally. Many web sites are aimed at the market of the jurisdiction where the physical business is located. Most businesses, especially small ones, do not put their servers offshore in order to escape

37. See Amelia H. Boss and Jane K. Winn, "The Emerging Law of Electronic Commerce" (1997), 52 Bus. Law. 1469.

38. See also G. Takach, *Computer Law, supra*, footnote 1, at c. 6, section C.2. See also Takach, "Internet Law: Dynamics, Themes and Skill Sets", *ante*, p. 1.

39. See http://www.law.ualberta.ca/alri/ulc/current/ejurisd.htm. See also Racicot, Hayes, Szibbo, and Trudel, "The Cyberspace is not a No-Law Land", http://strategis.ic.gc.ca/SSG/it03117e.html.

40. In March, 1999, the British Columbia Court of Appeal refused to enforce a Texas judgment for defamation on the Internet where the defendant and the corporate plaintiff were both in British Columbia: *Braintech Inc. v. Kostiuk*, http://www.courts.gov.bc.ca/jdb- txt/ca/99/01/c99-0169.txt. More connection with the jurisdiction was needed than availability on the Web, said the court.

41. For details of the American Bar Association's project on jurisdiction, see http://www.kentlaw.edu/cyberlaw.

local regulations.[42] Merchants may seek to inspire confidence in potential customers by making clear where they are located, *i.e.*, what laws they are subject to. People concerned about legal certainty will create a virtual community by dealing with merchants who create trusted environments, and legality is part of trust for that purpose.

It is important to note that many parties to electronic commerce will get their certainty from others, notably financial institutions. A merchant who wants to be paid may deal confidently with someone whose credit card number is confirmed with the bank. The credit card system is already global, resting on a network of local and transnational contracts, so it can function well in global commerce. In addition, further work is being done, as has been mentioned, in reference to the SET protocol. So long as the merchant trusts its own bank, the location of the customer is less important. To date the customers do not have the same trust-enhancing system on which to rely for the quality of the products to be bought. Some elements of the consumer's interest are discussed in a following section of this article.[43]

8. Intellectual Property

The main intellectual property problem for commerce on the Internet is the protection of copyright in a medium that allows for simple copying and undetectable distribution. It is disturbingly easy to destroy the economic return of the producer of copyrighted material. Some people have predicted that the rise of the Net spells the end of copyright in general.[44] Recently, however, the predictions are becoming less dire. Technology is starting to catch up and it lessens the ease of copying, or at least the ease of untraceable copying. In addition, technology may permit economic ways of billing very small amounts for the use of intellectual property. Putting a text on a web site will not necessarily mean in practice giving the whole world the ability to copy and distribute. It may become practical to charge each reader an economically attractive amount for downloading the text, subject to a (clickwrap) licence about its

42. See John D. Gregory, "Regulating Language on the Web" (1998), 2 Inform. & Techn. Law Bull. 50.
43. See Section IV(3).
44. See, for example, John Perry Barlow, "The Economy of Ideas: A Framework for Rethinking Patents and Copyrights in the Digital Age (Everything You Know about Intellectual Property is Wrong)", *Wired* (March, 1994).

uses. Repeated often enough, this process may give the creator a fair return on the effort made to produce it. Not everyone agrees that this technological fix can be made to work, however.[45]

The other area of intellectual property in electronic commerce about which one hears much discussion is trade marks, and in particular the relation between domain names, *i.e.*, electronic addresses on the Internet, and trade marks. Sally Abel's presentation at the 28th Annual Workshop on Commercial and Consumer Law dealt with this issue in detail, and I will not attempt even to survey the field.[46] There seems to be little Canadian experience with the disputes that she describes.[47]

9. Summary

Some traditional legal practices have come into question in the new world of electronic commerce. As businesses and consumers and courts become familiar with the problems, however, they often find ways, by agreement, by extension of precedent, or by technology,[48] to restore sufficient certainty to the legal effect of their relationships to allow them to carry on, and even prosper. Some areas are less amenable to private solutions of this kind, however. To those the article now turns.

III. STATUTORY BARRIERS TO ELECTRONIC COMMERCE

Sometimes the barriers to electronic transactions are not uncertainty, but rules that require things to be done on paper. One will

45. In addition, there may be public policy concerns about this solution. Current copyright law allows for free use of copyrighted materials for some purposes, such as academic study, criticism, and the like. If the micropayment system prevented these uses, they would shift the public policy behind the current balance of rights of copyright holders and potential users.

46. The most recent version of her frequently updated paper, "Trademark Issues in Cyberspace: The Brave New Frontier", is at the Fenwick and West web site, http://www.fenwick.com/pub/trademark_issues_in_cyberspace.htm. [Ms Abel's paper is not being published in this issue of the C.B.L.J. (ed.)]

47. See *ITV Technologies, Inc. v. WIC Television Ltd.* (1997), 77 C.P.R. (3d) 486 at p. 495, 139 F.T.R. 293 (T.D.). See also *PEINET Inc. v. O'Brien* (1995), 61 C.P.R. (3d) 334, 130 Nfld. & P.E.I.R. 313, though the case should be treated with caution. See G. Takach, *Computer Law, supra*, footnote 1, p. 123.

48. These three methods for accommodating electronic commerce within existing legal frameworks are part of George Takach's themes in his *Computer Law, supra*, footnote 1. See for example "Computer Law: Skill Sets" at pp 444ff.

note that the common law does not require commercial transactions to be documented on paper, and thus of course does not require documents to be signed.[49] Non-lawyers may confuse good business practices ("Get it in writing") with legal requirements ("It has to be in writing.") Tradition has accustomed people to dealing on paper, and to looking for signatures. Technology can replace tradition. Many businesses and governments are re-examining their usual ways of going about their work in order to accommodate electronic records with electronic signatures or other ways of ascertaining the origin of the records.

1. Evidence

When they do this, the most serious legal challenge may be one of evidence: will the courts accept computer-generated records to prove the legal relationships they purport to create? While the courts have generally accepted electronic records, some law reform has been directed at this problem too. In August 1998, the Uniform Law Conference of Canada adopted a Uniform Electronic Evidence Act,[50] which focuses on questions of authentication, the best evidence rule (the search for originals), and the relevance of recognized standards of record-keeping to the admissibility of the records. The Act is intended in operation to validate the common evidence provisions in trading partner agreements, whose enforceability has sometimes been doubted in academic and professional writing, though not so far in court. In October 1998, the government of Canada introduced amendments to the Canada Evidence Act based on the Uniform Electronic Evidence Act.[51] Ontario proposed the Uniform Act as an amendment to the Ontario Evidence Act in 1999.[52]

The Civil Code of Quebec that became effective in 1994 has provisions dealing with signatures and evidence that would support

49. The United Nations Convention on the International Sale of Goods provides that international sales contracts need not be in writing, unless a special declaration is made by a contracting state: see Articles 11 and 12. The convention is in force in Ontario under the International Sale of Goods Act, R.S.O. 1990, c. I.10. The text of the convention appears as a schedule to the Act.
50. See http://www.law.ualberta.ca/alri/ulc/acts/eeeact.htm.
51. Part 3 of the Personal Information Protection and Electronic Documents Act, Bill C-54. See footnote 33, *supra*.
52. Schedule B to the Red Tape Reduction Act, 1999, introduced on April 27, 1999 as Bill 12.

electronic dealings. The new definition of "signature" is in article 2827, and evidence provisions are articles 2837 to 2839. They deal with, among other things, the reliability of systems and the presumption of validity of evidence from third parties created in the ordinary course of business. New Brunswick passed an electronic evidence Act in 1996[53] which adds provisions to the provincial Evidence Act to deal with data evidence and electronic images.

2. Writing and Signature Requirements

However, many statutes do demand written records, or written evidence of transactions, or written notice. A number of statutes also require that documents be signed by the party legally responsible for the content of the documents. The most obvious traditional example is the Statute of Frauds[54] with a related provision in the Consumer Protection Act.[55] The Statute of Frauds requires a signed memorandum in writing to enforce a variety of legal obligations, such as guarantees, land transactions, and others. Until 1994 Ontario law also required a signed written memorandum to enforce a sale of goods for over $40 if delivery and payment were not immediate, or for contracts of any kind not to be performed for a year. The sale of goods requirement and the main contractual provisions of the Statute of Frauds were repealed in Ontario in 1994,[56] but equivalents remain in force in several other provinces.

Statutory writing "requirements" may be phrased in many ways besides the direct obligation. They may simply provide consequences for lack of writing or signature. They may provide positive consequences for the presence of a signature. They may require duplicates or certificates or seals that seem to presuppose paper. Other statutes may require that "original" records be submitted or retained for legal effect. Many statutes require people to retain records, whether or not original, to prove transactions or profits or other compliance with the law. These statutes are often phrased in terms applicable most readily to paper records.

Statutory rules can usually not be set aside at the will of the parties to commerce.[57] They need to be changed if they are undue

53. S.N.B. 1996, c. 52.
54. R.S.O. 1990, c. S.19.
55. R.S.O. 1990, c. C.31, s. 19.
56. S.O. 1994, c. 27, ss 54 and 55.
57. Trading partner agreements of the kind noted in footnote 8, *supra*, often attempt to avoid these requirements by a provision barring a challenge of any transaction based on failure to comply with the requirements. It is not clear that such "opt out" provisions are

barriers to the way business must be carried on to be competitive, and to the way government must be practised if it is to be efficient.

3. Law Reform: Individual Efforts

A number of reform measures have been taken over the years to address these barriers. Many of them have applied to the government's use of electronic technology to ensure the proper authority for public activities. For example, Ontario's taxation statutes generally authorize the use of electronic records and give the same weight to printouts of the database as the law does to paper equivalents.[58] The Public Guardian and Trustee Act[59] allows the Public Guardian and Trustee to make electronic images of documents submitted to that office, destroy the originals and use the images with the same effect as the originals.

Governments have also addressed the interaction of the public with government institutions, particularly business applications. The Electronic Registration Act (Ministry of Consumer and Commercial Relations Statutes), 1991[60] has authorized electronic filings under the Personal Property Security Act[61] for several years, and more lately, filings under the Repair and Storage Liens Act[62] as well. The Business Regulation Reform Act, 1994[63] permits the submission of many documents in electronic format or by electronic transmission. It also allows government officials to dispense with signatures in appropriate cases. Amendments to and regulations under the Provincial Offences Act[64] permitted creation and court filing of photoradar speeding tickets in electronic form, including electronic proof of ownership of the vehicle from the records of the Ministry of Transportation.[65] Electronic land registration has been authorized by statute and regulation,[66] though the system is operating in only

valid. For further discussion, see Takach, *Computer Law, supra*, footnote 1, at pp. 347-48.

58. See the Corporations Tax Act, R.S.O. 1990, c. C.40, ss. 93(6.1) to (6.3), added by S.O. 1994, c. 14, s. 42(1). Ontario statutes and regulations are on line at http://legis.acjnet.org, as are those of the federal government and several other provinces.
59. Section 10.2 of the Act, R.S.O. 1990, c. P.51, as inserted by S.O. 1997, c. 23, s. 11(5).
60. S.O. 1991, c. 44.
61. R.S.O. 1990, c. P.10.
62. R.S.O. 1990, c. R.25.
63. S.O. 1994, c. 32.
64. R.S.O. 1990, c. P.33.
65. See O. Regs. 497/94 and 499/94.
66. The Land Registration Reform Act, R.S.O. 1990, c. L.4.

one county as of the spring of 1999. Rules of Civil Procedure under the Courts of Justice Act[67] permit electronic filing of civil action documents in Toronto, generally without signature (though proof of service of originating documents must be kept on paper in the lawyer's office and produced on demand).[68]

Without pretence of comprehensiveness, one might mention as well specific statutes from other provinces that support electronic filing or dealings with government. Nova Scotia has passed its Business Electronic Filing Act;[69] Saskatchewan has the Electronic Filing of Information Act,[70] and British Columbia enacted the Business Paper Reduction Act in 1998 as well.[71] The national system of filing disclosure documents with securities regulators across the country allows for electronic filing in the SEDAR system,[72] again without signatures (but the key documents must be held in signed form in the submitting lawyer's office and presented on demand, a feature shared by the similar EDGAR procedure of the Securities Exchange Commission in the U.S.[73])

It is worth noting that governments do sometimes re-examine the current process when they legislate. Just as private parties may decide to abandon traditional procedures when they go electronic, governments are deciding to do without signatures or other forms of paper-based documentation when the policy permits. In Ontario, people registering business styles[74] or partnership names can fill out paper forms; their signatures are never verified. The electronic filing of these forms, which now accounts for more than half of them, does not require a signature at all.[75] The principle is that there is little risk in not verifying origin of the applications. Registrants are not entitled to any benefit from the state that would require a serious effort to combat misrepresentation.

The Ontario government has also rolled out a number of "kiosks", computerized work stations through which one can renew

67. R.S.O. 1990, c. C.43.
68. See O. Reg. 288/99, revising R.R.O. 1990, c. 194.
69. S.N.S. 1995-96, c. 3.
70. S.S. 1998, c. E-7.21.
71. S.B.C. 1998, c. 26.
72. See http://www.sedar.com.
73. See http://www.sec.gov/edgarhp.htm.
74. Business styles are names other than the formal legal name under which legal or natural persons carry on business with the public. Registration is intended to let the public know who the suable person behind the name is.
75. The legal authority is found in the Business Regulation Reform Act. See O. Reg. 442/95, s. 3.

driver's licences, obtain licence plate stickers, and pay traffic fines, using a credit card for payment. To get a plate sticker, one must certify that one has valid auto insurance. At the kiosk, the certificate is a kind of clickwrap contract. The language of the certificate appears roughly as "I certify that the above information [on previous screens] is correct and I know I am subject to penalties if I misstate the facts." The legal authority is stated, the Compulsory Automobile Insurance Act.[76] Then one touches the screen on a button reading "I agree". (There is another button to provide a way out if the user does not wish to agree at this point.) There do not appear to have been any prosecutions to date based on a false statement at a kiosk, but the defendant would have a hard time showing any mistake of intention or effect.[77]

Less frequently, governments have removed form requirements that apply mainly or exclusively to the private sector. Ontario's repeal of parts of s. 4 of the Statute of Frauds and s. 5 of the Sale of Goods Act in 1994[78] was a rare example. It appears likely that the best hope for removal of statutory barriers to private electronic commerce lies in generic reform based on harmonized approaches to the problems.

4. Law Reform: Harmonized Approaches[79]

(A) United Nations Model Law on Electronic Commerce

Global electronic commerce has brought with it global legal problems. The nations of the world have been working together to resolve them. One of the most influential initiatives is the United Nations Commission on International Trade Law's Model Law on Electronic Commerce, adopted in 1996.[80] The Model Law has

76. R.S.O. 1990, c. C.25.

77. The person certifying has by this time already provided his or her credit card, verified by the machine on the spot, and details about licence number, vehicle serial number, and insurance policy number. The form was established under O. Reg. 278/95, which says that "a certificate of insurance required by subsection 13(1) of the Act may be in an electronic form approved by the Minister of Finance".

78. S.O. 1994, c. 27, ss. 54 and 55.

79. For a more comprehensive view of what is happening with many international organizations, see the OECD's report published at the time of the Ottawa Ministerial Conference in October, 1998. The document appears to have been taken off line. For international legislation, see the Internet Law and Policy Forum reports at http://www.ilpf.org.

80. The Model Law is at http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm. UNCITRAL also adopted a Model Law on Credit Transfers, found at the same web site, which borrows to some extent from Article 4A of the Uniform Commercial Code in the U.S. on electronic funds transfers.

three main sections. The first section, which appears in Chapter II, following definitions and formalities, provides a mechanism for solving writing and similar requirements for electronic messages. Chapter III provides rules for communications, particularly pertinent to electronic contracting and the role of intermediaries. The third section (Part Two of the Model Law) deals specifically with the carriage of goods. The Model Law was left open for additional provisions as technology required and the ability of the members of UNCITRAL to reach consensus permitted.

The first section is perhaps the most important. It does not try to redefine traditional paper concepts like writing and signature and original to include electronic records. This approach would be problematic because of the practically unforeseeable applications of these concepts. If writing is defined to include electronic communications, electronic communications would have to work for all purposes for which writing is required. That may be too broad.

Instead of proceeding by definition, the Model Law looks for "functional equivalents" of paper records. An electronic message or record (the general term in the Model Law is "data message") that fulfils the "policy" function of written records is said to satisfy the legal rule that requires paper. Thus Article 6 provides that where a rule of law requires writing, that requirement is satisfied by a data message if the information in it is accessible so as to be usable for subsequent reference. Likewise Article 7 says that where a rule of law requires that a record be signed, that requirement is satisfied if a method is used to identify the person signing the record and to indicate his or her approval of the record, and if the method used is as reliable as was appropriate in the circumstances, including the existence of any agreement between the parties.

One will note that the Model Law's standard is fairly vague. It does not say exactly how the functional equivalent is to be created. As a result, some attempts to meet the standard may fail, or at least result in litigation. However, this is inevitable in such a fluid area as the use of technology to manage documents. There are so many possible ways to create a record and to secure it and to attribute it to its originator, that a statute that tried to spell out how to create the document or signature electronically might prove too restrictive. The Model Law does have the virtue of opening up wide fields for agreement on standards. As between themselves, parties to such agreements on the conduct of their electronic commerce

will be confident that they have satisfied the statutory requirements and that their transactions will not be challenged by the other party.

Further provisions of Chapter II deal with how to satisfy requirements for original records, with admissibility and weight of electronic records offered in evidence, and with record retention rules. The former and latter put much weight on demonstrating the continued integrity of the content of the electronic record as a substitute for its originality (a concept not readily applicable to most electronic records) or for physical custody of the record. The evidence provision prohibits refusal to admit an electronic record solely because it is electronic or because it is not the original record if it is the best evidence available. It then lists factors that courts should consider in weighing electronic evidence: the manner of generating, storing or communicating the record, its maintenance, the identification of the originator, "and to any other relevant factor".

The Model Law recognizes that many countries will be uncomfortable with the prospect of electronic records being used for all purposes. Most of the provisions of Chapter II therefore allow for exceptions, cases in which the general rule that a data message satisfies the requirement for writing, or signature, or original does not apply. This is a useful safety valve that would be harder to draft if one were to try to solve the problems by defining them away. However, the Model Law does not actually fill in the blanks. It lets each enacting country decide what it wants in or out. This makes excellent sense for an international body seeking consensus, but it leaves member countries to decide the scope of their own legislation without a lot of guidance. We will return to this subject in considering the Canadian experience with legislation.

The influence of the Model Law has been widespread. This article will look quickly at its implementation in common law jurisdictions, then spend more time on Canadian initiatives inspired by it.

(B) Singapore

The first country in the world to put the Model Law into effect was Singapore, whose Electronic Transactions Act was passed on June 29, 1998.[81] That Act drew inspiration as well from several

81. See http://www.cca.gov.sg/eta/index.html.

American models that will be mentioned shortly.[82] Singapore distinguishes between private records and records to be submitted to or generated by government. Government records are dealt with more restrictively, in that the general enabling rules do not apply to them until the government so decides. Part II of the Singapore Act picks up much of Chapter II of the Model Law: the general non-discrimination rule (not to deny legal effect to a record solely because it is in electronic form) and the writing, signature and record retention rules. Evidence is in a separate statute in Singapore. Requirements for original records were omitted from the Act, on the ground that such requirements arose only in the law of evidence, which was already provided for; in the law of negotiable instruments, which was excluded from the Act; or in dealings with government, which had their own part.[83] Part IV of the Act implements much of Chapter III of the Model Law under the title "Electronic Contracts".

(C) Australia

Australia has also shown much interest in legislating on electronic commerce. An Attorney General's Expert Group on Electronic Commerce reported in March, 1998, that legislation should implement the Model Law with few changes.[84] A draft statute was published for comment in January 1999.[85] Such legislation should ideally be uniform across the country. Australia has a Uniform Evidence Act, now in force in the Commonwealth and in New South Wales, that removes the need to deal with the evidence provisions of the Model Law. The state of Victoria has published draft legislation on electronic signatures that is much influenced by the Model Law as well.[86] Victoria has said that it will defer to national legislation if such legislation is passed in the future.

---

82. Notably the Massachusetts Electronic Records and Signatures Act, http://www.magnet.state.ma.us/itd/legal/mersa.htm (November 1997 draft) and the Illinois Electronic Commerce and Security Act, http://www.ag.state.il.us/resource/cecc/cecc2.html. (For comments, see http://www.mbc.com/eceemsg.html.) Notes in the first reading version of the Singapore statute also cite as sources the Uniform Electronic Transactions Act, described in Part III(4)(d) of this article, and the Utah Digital Signature Act, Utah Code Annotated title 46, Ch 3 (1996).
83. Conversation with member of Singaporean drafting team, July 1998.
84. See http://www.law.gov.au/aghome/advisory/eceg/ecereport.html.
85. See http://www.law.gov.au/ecommerce.
86. See http://www.mmv.vic.gov.au, under "Publications". At the same site is a draft statute on the protection of privacy. Both are .pdf files.

(D) United States

Harmonized law reform has been sought in the United States as well. Most states have some kind of legislation on electronic records or electronic signatures, but many of them are empty, in that they simply appoint a commission to study the question further or give a state agency the power to make regulations permitting electronic business in due course. Some are limited to specific sectors, such as health records.[87] Among the states with substantial laws or proposals which are most influenced by the Model Law are Illinois, which passed the Electronic Commerce Security Act in August, 1998[88] and Massachusetts, which has published a draft Electronic Records and Signatures Act.[89] Others, notably Utah and California, have pushed further into specific technology on signatures; their legislation will be discussed in more detail in the next section of this article.[90]

On a national basis, efforts have been underway for a decade to update parts of the Uniform Commercial Code to take account of electronic commerce, among other matters.[91] Article 4A is devoted exclusively to electronic funds transfers among financial institutions. Article 8 now deals with electronic settlement of transfers of investment holdings in a market that rarely sees the transfer of share certificates. Article 5 contemplates electronic letters of credit and supporting documents. Revisions to Article 2, still in draft, pick up some Model Law concepts in the law of sales. The most far-reaching effort in the UCC in this field was to be the proposed new Article 2B on software and information licensing.[92] Many of its provisions are inspired by the Model Law, both Chapter II and Chapter III concepts.

87. For a review of state activity in this field, see http://www.mbc.com/ds_sum.html. For another analysis of themes of this activity, see http://www.perkinscoie.com/resource/ecomm/digsig/state.htm.
88. See *supra*, footnote 82.
89. *Ibid.*
90. See *infra*, Section IV(1). Texas and Florida are others with some originality in their legislation. All can be traced through the www.mbc.com web site mentioned in footnote 87.
91. The Uniform Commercial Code, or UCC, is the product of the National Conference of Commissioners on Uniform State Laws (http://www.nccusl.org) and The American Law Institute (http://www.ali.org). Draft articles of the UCC are at http://www.law.upenn.edu/library/ulc/ ulc.htm. For the developments on electronic commerce, see Boss and Winn, *supra*, footnote 37.
92. Now the proposed Uniform Computer Information Transactions Act. See the more detailed discussion below at Section IV(2). Also see http://www.2bguide.com.

Beyond the Uniform Commercial Code the harmonization efforts are concentrated in the work on the Uniform Electronic Transactions Act, also a product of the National Conference of Commissioners on Uniform State Laws.[93] The UETA clearly draws its strengths from the Model Law.[94] Indeed, over the course of its drafting history since the spring of 1997, the UETA has been stripped of many of the provisions that attempted to go beyond the Model Law. When it reaches its final form, now foreseen for the July 1999 annual meeting of the national conference, it may have little left but the Model Law provisions. It does, however, contain a special part on government records, with a similar effect to Part XI of Singapore's Act.

All of these initiatives have focused on state law. Some bills have been presented to the U.S. Congress as well.[95] They have tended to focus on use of electronic records or signatures by the federal government,[96] though some have been broader.[97] They have not aimed at general reform of commercial law. To date few have attracted enough support to pass, though some have generated interesting testimony in committee about the goals of law reform on this topic.[98] Some of the administrative work at the federal level has been effective as well.[99]

93. See drafts at http://www.law.upenn.edu/library/ulc/ulc.htm#ueccta.
94. A history of the relationship between U.S. law and the United Nations work is found in Amelia H. Boss, "Electronic Commerce and the Symbiotic Relationship between International and Domestic Law Reform" (1998), 72 Tul. L. Rev. 1931.
95. See http://www.ilpf.org/digsig/federal.htm for a list, including administrative regulations on electronic signatures, such as those of the Food and Drug Administration.
96. The Government Paperwork Elimination Act was passed in October 1998. The Act is at the site noted in the previous footnote. Draft implementing regulations were published on March 5, 1999. See http://www.cio.gov/ or http://www.whitehouse.gov/WH/EOP/OMB/.
97. A bill with fairly broad support was introduced in the Senate and House in March 1999 under the name Millenium Digital Commerce Act. See http://www.senate.gov/~abraham/mdcat.htm. The operating provisions of the Act pick up Model Law principles of non-discrimination against electronic contracts in interstate commerce, and the freedom of contracting parties to design their own signature systems.
98. See, for example, the proceedings of the U.S. Senate Banking Committee on October 28, 1997 at http://www.senate.gov/~banking/97_10hrg/102897/index.htm.
99. See, for example, the Food and Drug Administration's detailed rules on electronic signatures at http://www.fda.gov/cder/esig/part11.htm (amending 21 C.F.R. Part 11).

(E) Canada[100]

(i) Uniform Electronic Commerce Act

(a) General

In Canada, the main effort at harmonizing law on electronic commerce is being conducted through the Electronic Commerce project of the Uniform Law Conference of Canada.[101] Among its priorities is to implement the Model Law in Canada. Its first step in doing this is drafting the Uniform Electronic Commerce Act, which was discussed at the annual meeting of the conference in Halifax in August 1998.[102]

Like the American and Singapore statutes, the UECA has separate parts for general records and for government records. The intention is to give the government more control over the use and particularly the inflow of electronic information, for fear of being swamped by the amount of information and the variety of possible formats. Governments do not have contracts with most of the citizens or residents of the country, so they are unable to protect themselves by making reasonable requirements by agreement. They need legal authority, not in order to create barriers but to build guidelines.

Part 1 of the UECA deals with the provision and retention of information. It contains the non-discrimination clause, basically Article 5 of the Model Law: "Information shall not be denied legal effect solely on the grounds that it is in the form of an electronic document." The commentary notes that this is the basic principle of the Act. The part provides for the satisfaction of statutory requirements by electronic documents.

Section 5 deals with a requirement to provide information, and says that the electronic document must be under the control of the

100. This article omits two early Canadian texts influenced by the U.N. Model Law. Ontario's regulations for photoradar filing were consciously patterned after thinking in the then current draft of the Model Law: see John D. Gregory, "Electronic Documents in Ontario's Photoradar System" (1995), 6 J.M.V.L. 277. The Offence Act of British Columbia was amended in 1997 to incorporate provisions resembling articles 6 (writing requirements) and 7 (signatures) of the Model Law: see S.B.C. 1997, c. 28, s. 13.

101. For information about the Uniform Law Conference, see http://www.law.ualberta.ca/alri/ulc/eindex.htm. Since 1993 the conference has been considering the impact of the use of information technology on the basic laws of Canada, mainly in the fields of evidence and commercial law.

102. See http://www.law.ualberta.ca/alri/ulc/acts/eueca-a.htm for an annotated version of the March 1999 draft. Texts from 1998 are at the same site at /ulc/current/euecaa.htm and /ulc/current/eee98il.htm, the latter for an overview of the purposes of the Act.

person to whom it is provided and the information contained in it must be accessible so as to be usable for subsequent reference. The control feature here is added to the Model Law's Article 6. The UECA drafting team thought that the Act should more closely replicate the status of a paper document. While the document need not have permanence, and the recipient may destroy it, nevertheless the recipient should have that choice. As the 1998 commentary says, "putting a notice on one's own Web site would not satisfy a provision that one must give notice in writing, at least until the intended recipient downloads it." The commentary continues:[103]

> The draft Act is silent on provisions of law that simply require someone to provide information, without saying anything about the form of the information. Under such a provision one could use electronic documents today. To the extent that there is any doubt, section 3 should resolve it by ensuring equal legal effect to electronic documents in the absence of specific rules that would deny the effect.
>
> The draft Act does not allow parties to opt out of the standards in Part 2, except where specifically provided. Section 8 on signatures allows a court to take account of an agreement, though the agreement would not be definitive. The reason for the limit is that these rules tell people how to satisfy provisions of law; they are not allowed to opt out of rules of law any more electronically than they would be on paper (or any less).

Section 6 deals with prescribed forms and has similar rules to s. 5 on writing, plus the information has to be presented in a form substantially similar to the prescribed version.

Section 7 states how one satisfies a demand for originals, in much the same language as Model Law Article 8. Section 8 is the signature rule. In the words of the 1998 Commentary:[104]

> This rule originates in Article 7 of the Model Law. However, the Model Law requires that the person signing should choose a method that indicates the person's "approval" of what is signed. The working group took the view that the legal effect of the signature should be left to the general law, and that the element of approval was not essential to the function of the signature. The element of identification and association in some way, for some purpose, was essential.
>
> The draft Act indicates how the signature may be connected to the document, i.e. it may be "incorporated in, attached to or logically associated with" it. This is intended to cover rather than describe all the methods of signing electronically.

103. See http://www.law.ualberta.ca/alri/ulc/current/euecaa.htm at s. 6.
104. See http://www.law.ualberta.ca/alri/ulc/current/eueca.htm at s. 8. The language has evolved in later drafts but the principle remains the same.

The working group left open for discussion whether one needed to specify the intent of the person whose identity was being associated with the document. It is arguable that the term "signature" itself does that work. The 1999 draft of the UECA has added a definition of electronic signature, so that no one is misled into thinking that an electronic signature has to "look like" a handwritten signature; a series of codes or sounds or an encryption can function as a signature. (In Ontario's photoradar ticket system, a series of photographs taken in a particular sequence constituted part of a signature.[105])

Section 9 deals with record retention, again much as in Article 10 of the Model Law, but adding that the record must remain accessible for the period for which the retention rule requires it to be retained. It is beyond the scope of the UECA to say just how this is to be done in a time of quickly evolving and quickly obsolescent storage techniques and degrading storage media. If storage is beyond the record manager's ability, then it may be unsafe to try to retain electronic records for the required period.

Part 2 of the UECA is called "Communications with Government". It contemplates that rules about submitting information to government or handling information in government will be listed in schedules when the responsible minister is comfortable that the program area is able to handle the information electronically. At the time of the designation of the program (or the statute or the regulation), the minister is to make rules about how the electronic documents are to be dealt with by the program. In short, the Act has no effect until a minister opts into it. This schema is adopted for writing, original, and signature requirements. In addition, s. 15 makes similar provision for a requirement to submit copies. Section 16 contains a list of rules about statutory or prescribed forms. Section 17 permits payments to or by government by electronic means.

The UECA was adopted in principle in August 1998, and the working group was asked to come back to the member jurisdictions (the federal, provincial and territorial governments) with a list of questions and revisions to take account of the discussion in Halifax. The working group is considering two questions in particular. The first concerns the scope of the Act, *i.e.*, what should be exempt from it? The second concerns the role of consent in enabling electronic records to be used.

105. See Gregory, *supra*, footnote 100.

(b) Exemptions

As noted earlier, the Model Law contemplated exceptions to its application but did not say what they should be. Each enacting country has to decide what its policies support, or what its legal system or its citizens will be comfortable with. The Guide to Enactment of the Model Law says, in para. 9:[106]

> [T]he objectives of the Model Law are best served by the widest possible application of the Model Law. Thus, although there is provision made in the Model Law for exclusion of certain situations from the scope of articles 6, 7, 8, 11, 12, 15 and 17, an enacting State may well choose not to enact in its legislation substantial restrictions on the scope of application of the Model Law.

Three main approaches to this question have emerged. Two prescribe exceptions from a statute of general coverage; the other makes the statute apply only to specified rules of law. The working group came to describe these as the opt-out and the opt-in approaches.

The provisions on government documents in the UECA represent the opt-in approach. Nothing is covered unless it is designated. This allows for consideration of the particularities of every functioning program or law and the devising of rules to cover their electronic equivalents. It is argued in favour of this approach that many areas of law have their own complexities that require careful examination in the creation of a generic statute. As a result, one might as well keep to the safe path and make a conscious decision to apply the Act or not to apply it. On the other hand, it was submitted that this would slow the growth of electronic commerce, despite the demands for legal certainty from business and government alike. Some people feared that the failure of the government to opt in a particular rule of law would be interpreted as a rejection of the right to use electronic documents to satisfy that rule. The "enabling" statute should at the very least not chill electronic commerce!

The first of the "opt out" approaches is to leave the exceptions at the level of principle: would the use of electronic records to satisfy a particular rule — a writing or signature requirement, for example — violate the fundamental principle behind that rule? Would the permission to go electronic be "repugnant" to the policy

106. See http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm, "Guide to Enactment", at para. 9.

of the rule? The draft Massachusetts statute took this approach.[107] The Illinois Act used it as a general statement leading off a list of more specific exceptions.[108] The early drafts of the UETA used the Massachusetts language, but then dropped it. The repugnancy test was criticized as too vague and thus uncertain; people would not know at the time of their dealings whether the enabling statute covered them or not.[109] It was also felt that if the result of applying the general statute was really egregious or repugnant, a court would find a way to provide appropriate relief.

The second of the "opt out" approaches lists specific exceptions to which the general permissive statute simply does not apply. Singapore used a short list: the creation or execution of a will; negotiable instruments; trusts (except constructive and resulting trusts as they are not privately created documents but remedies imposed by a court); contracts for the disposition of immovable property; documents of title.[110] The UECA has a similar list: wills, trusts, powers of attorney; negotiable instruments and (negotiable) documents of title; dealings in land and interests in land.

After the National Conference's Drafting Committee decided to drop the repugnancy test from the UETA, in January 1998 it set up a task force on scope and exclusions. That task force reported in September 1998.[111] It recommended very few exclusions: wills and codicils, personal trusts created by testamentary instrument; jurats and declarations used in court filings and sworn testimony. Otherwise it wanted the UETA to cover everything. The reasoning in many cases is that the law did not provide any form requirement for paper, and sometimes did not even require paper at all — as in the creation of a trust or an agency relationship — so it should not restrict the form of such documents electronically. It qualified its report so far as negotiable instruments were concerned, saying the subject needed further study, but the UETA should proceed with drafting its provisions on what it calls "transferable records" (records that would be

107. See the Massachusetts Electronic Records and Signature Act, *supra*, footnote 82.
108. See the Electronic Commerce and Security Act, *supra*, footnote 82, for example in s. 5-115.
109. See reports of the Drafting Committee meetings at http://www.webcom.com/ legaled/ ETAForum. The repugnancy provision was discussed at the January 1998 meeting and again in October 1998.
110. See the Singapore Act referred to at footnote 81, *supra*.
111. Its report can be found at the ETA Forum web site referred to in footnote 109, *supra*.

chattel paper or documents of title if they were in writing) in case a workable rule could be found.[112]

The task force also dealt with a subject that the UECA team has had to return to: the relationship with other statutes that already contemplate electronic documents to some extent. Should the generic statute replace them or complement them or simply not apply, conceding the field of policy and operations to them? In the United States, the discussion has largely focused on the relationship between the UETA and the UCC, which, as noted earlier, has several articles prepared with electronic documents in mind (though some articles have them more thoroughly in mind than others).

The Canadian discussion has not yet taken a sharp focus. Section 11 of the 1998 draft of the UECA, in the part concerning government documents, allowed a minister to use electronic means to create documents "even if a law . . . does not specify how that thing is to be done *or specifies that the thing is to be done by other than electronic means*" (emphasis added). One can see the appeal of this language, to avoid old-fashioned provisions which used terms like "writing" on the assumption that people would always communicate in that manner. To that extent it merely reflects for outgoing or internal documents the rule for private sector writing requirements or incoming records. However, the italicized clause would also negate a provision passed by the legislature in full contemplation of the possibility of using electronic records where it decided to restrict documents to paper. One might consider the fate of the exceptions under the UECA itself. If the legislature excludes wills from the permissive statute, why should anyone else have the authority to add them back? For this reason the current (March 1999) draft has dropped the italicized words.

The scope provisions in s. 2(1) now also exclude rules of law that make express provision for electronic records. In addition, power to exclude further rules by regulation has been added, as has been done in Singapore and in the draft Australian legislation. While this adds uncertainty to the scope, it reduces the risk of unintended consequences of the general permission of the UECA without the need to count on remedial legislation.

(c) Consent

One of the concerns expressed about the "opt out" approach is that the permissive statute would permit too much, *i.e.*, that it

112. See the discussion on negotiability above in Part II(5).

would force people to accept electronic records when they were not ready to do so. One example given to the working group was the insurance industry. Proofs of claim for payout on insurance are to be delivered in writing. Could policyholders on the first day of the new statute submit claims by e-mail? What would stop them? What if the insurance company was not ready? This is similar to the issue that led to the creation of a special section for government documents.

A safeguard against that result is found in s. 4 of the UECA: "Nothing in this Part requires a person to use or accept information in the form of an electronic document." The UETA provides similarly in s. 104(a): "This Act does not require that records or signatures be generated, stored, sent, received, or otherwise processed or used by electronic means or in electronic form."[113] It goes without saying that one can impose conditions on one's consent without regard to the later statutory requirement that they be reasonable.

The Canadian working group and the annual meeting have both debated the relationship between s. 3 of the UECA — "information shall not be denied legal effect solely on the grounds that it is in the form of an electronic document" — and s. 4, the consent principle. It is thought that s. 4 gives anyone the right to deny legal effect to a document solely on the ground that it is in electronic form. Parties can agree that electronic documents are acceptable but, in the absence of an agreement, it may not be safe to rely on the UECA for permission to communicate electronically.

The 1999 draft makes clear that parties may agree by conduct to accept electronic records. However, merely having the capacity to accept them is probably not enough. The secured creditor who intends to seize the debtor's property and who must give notice to other creditors with an interest in the collateral may not give that notice electronically just because it managed to discover their e-mail addresses.

These considerations impose a fairly restrictive term on the permission. Anyone creating a document intended to be good against the world, like the settlement of a trust or a power of attorney, may need to stay on paper to meet the requirements of a counterparty who refuses to accept it in electronic form. With a durable power of attorney, or some trusts, or a will, the originator

113. All quotations from the UETA are taken from the March 1999 draft, http://www.law.upenn.edu/library/ulc/uecicta/eta399.htm.

may not be available or competent to make a paper version of the document if the electronic version is not accepted. It would be safer to keep to paper in the first place.

The Model Law does not limit its application based on the consent of the parties to communicate electronically. On its face, the first part of the Model Law provides that electronic messages complying with its provisions will meet legal requirements, whether the recipient of an electronic message asks to receive it electronically or not. As noted earlier, the Model Law does not attempt to spell out exceptions to its application, but such a factor could be important in deciding what to omit. The Singapore statute[114] is also silent on consent. The ULCC working group is inclining to confirm the implication in the draft UECA that consent is needed for electronic records to be given legal effect. As a result, the scope of the Act is narrower than it may appear. There may, however, be ways to show that standard practices of receiving electronic records constitute consent, so one is not faced with random, arbitrary or surprising refusals.[115]

Another question that arises about consent is how real the consent must be. In a world of standard form contracts, one imagines large organizations putting into their contracts an agreement to use electronic communications. Will this be fair to all the other parties? What risks are built in, or assumed, in the description of the systems that the parties "agree" to use? The Australian report[116] recommended some safeguards to protect the vulnerable against disadvantageous agreements. The UETA, building on Article 4A, provided until recently that a party that imposes an "unreasonable security procedure" (essentially a way of checking identity of the originator and the integrity of a record) may not enforce against the other party an agreement to be bound by the results of that procedure.[117] So far, the Canadian working group has not decided to

114. The Electronic Transactions Act. See footnote 81, *supra*.

115. Article 5 of the Uniform Commercial Code in the United States, dealing with letters of credit, allows for electronic documentation on consent of the parties or where standard practices of the parties involved include the use of electronic documents: UCC, s. 5-102(a)(6).

116. See *supra*, footnote 84. The draft Australian statute referred to in footnote 85 does not contain such safeguards.

117. The language about unreasonable security procedures was removed from the UETA after the October 1998 meeting. As of April 1999, the statute retains few express rules relating to the fairness of the allocation of risks from the nature of electronic communications.

impose such a limit. The general law of contract may provide sufficient recourse for unfair terms.

(ii) Personal Information Protection and Electronic Documents Act

On October 1, 1998, the federal government introduced Bill C-54, the Personal Information Protection and Electronic Documents Act.[118] Part 2 of the bill deals with electronic documents. Many of the 21 sections of this part are similar to those of the government documents part of the UECA, as there was overlap in the project teams and the same legislative counsel drafted both statutes. The federal approach is permissive and opt-in. Its purpose is "to provide for the use of electronic alternatives in the manner provided for in this Part where federal laws contemplate the use of paper to record or communicate information or transactions".[119]

Bill C-54 allows ministers to do things electronically "whenever a federal law does not specify the manner of doing so". In other words, it does not allow the minister to override provisions that do specify the manner, as did the UECA in 1998.

Because Bill C-54 is an opt-in statute, it does not face the question of scope or exclusions. If policy does not support doing statutory things electronically, the government simply will not designate those things under the Act. The Act and the surrounding explanatory material[120] do not describe the reasoning that will support or counter a decision to opt in for any particular statute. The criteria will be in part pragmatic — can we afford to handle electronic records? are we ready? — and in part principled. Perhaps the Parliamentary debates will reveal some of the principles that the ULCC might use to define its exclusions. As noted, the federal government has been an active member of the working group on the UECA project. Its role there and the influence of the statute are likely to be such that Bill C-54 qualifies as an example of "harmonized law reform", and not just as an "individual effort".[121]

---

118. See *supra*, footnote 33. Second Reading was completed on November 3, 1998.
119. Bill C-54, s. 32.
120. See http://canada.justice.gc.ca/Ecommerce/ for the press release and backgrounders.
121. The work of Industry Canada's Electronic Commerce Task Force is described at http://e-com.ic.gc.ca/, which site also has links to provincial and territorial initiatives.

5. Summary

Some electronic commerce practices inevitably run up against old statutes that require the use of paper, either because characteristics of paper were valuable, such as permanence, reproducibility, transferability and the like, or because that was the only conceivable way to talk about things when the statute was drafted. Some of the values of these statutes may still require paper, but many can be satisfied by electronic means. The challenge is to legislate these means as economically as possible, ideally without rewriting most of the statutes in the statute books, while preserving the values that need preserving. It is tempting, particularly for governments but also for interest groups, to look for special enactments to open doors for themselves. Electronic commerce would be better served in most cases by more general legislation to ensure common approaches to these common problems. Devising these common approaches and having them accepted will sometimes be difficult. Acceptance requires a fairly broad level of comfort with how the technology works and what it can do, and people arrive at this comfort level differently and at different times.

IV. PROMOTING ELECTRONIC COMMERCE

This article has examined some of the areas of legal uncertainty presented by electronic commerce and the ways that business lawyers are working to reduce them by private means. It has also dwelt on statutory removal of traditional legal rules that created barriers to electronic commerce. The third area where law and e-commerce intersect is the set of statutes designed to go beyond the removal of uncertainty or of barriers to actively promote doing business electronically. The border between these categories is admittedly not a bright line, but the policy impact of all of the examples that will be explored here is arguably broader than just clarifying the law or getting statutory barriers out of the way of the new technologies.

1. Enhanced Signatures

It was noted in the discussion of Article 7 of the Model Law that its standard is vague: the signature method must be as reliable as is appropriate in the circumstances, "including any relevant agreement". The presence of an agreement is not definitive but

only one factor to be considered. Some people would like to go beyond this to achieve greater certainty. They argue that some technologies permit great confidence in the ability of electronic methods to ensure what a signature has to ensure: identity of the originator of the message. Likewise, some writing requirements are said to be so important that better technology is needed to meet their demands.[122] If such trusted technology is used, and especially if it is used by agreement, then it is argued that the law should reward the users with enhanced or more certain legal effects. At least two or three quite different effects have been suggested: that the trusted signature be given the same legal status as a handwritten signature, *i.e.*, deemed to be appropriately reliable; that the apparent signer be presumed to be the actual signer and thus liable as if he or she had signed; or that the owner of a trusted signing device should be responsible for any misuse of the device due to the owner's carelessness.

Much of the early discussion of these possibilities arose because of the confidence of the proponents of digital signatures in the effectiveness of public key cryptography.[123] Digital signatures are created by encrypting a message code using the private key of a pair of keys that are related mathematically. The recipient decrypts the message code with the public key of that pair. There is effectively no chance that a message could be decrypted with a public key that was not associated with the private key. Therefore, one can have great confidence that the "signed" message came from the holder of the private key. One knows who that is because, in the usual scenario, a "trusted third party" has certified the identity of the holder of the private key. In bilateral trade, the parties may exchange keys by trusted means, including direct transfer in person.[124]

---

122. This argument has been made in the context of digital signatures in the current round of UNCITRAL discussions on electronic commerce.
123. For an on-line tutorial on the use of digital signatures, see American Bar Association, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.htm. The guidelines are at http://www.abanet.org/scitech/ec/isc/dsgfree.htm.
124. One of the controversies in legislating in this area is knowing what the "usual" scenario is. There are no open-system public key infrastructures now in operation. The outlook of the ABA Guidelines and the early statutes was the trusted-third-party setup: see Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce" (1996), 75 Oregon L. Rev. 49, http://www.law.miami.edu/~froomkin/articles/trusted.htm. Several other relationships are also imaginable. See, for example, D. Masse and A. Fernandes, "Economic Modelling and Risk Management in Public Key Infrastructures" at http://www.chait-amyot.ca/docs/pki.htm.

The State of Utah passed its Digital Signature Act in 1995[125] and was the first state to give full legal effect to digital signatures supported by certificates issued by a trusted third party, or certification authority, licensed by the state. Since then several other states have passed similar laws.[126]

However, some were nervous about legislating for a single technology, no matter how impressive. Efforts arose to prepare a "technology neutral" version of the enhanced signature law. California was first off the mark, giving enhanced status to "electronic signatures" certified by the Secretary of State.[127] The Illinois statute mentioned earlier[128] was influential in its terminology as well as in its principles. It made definitive the term "secure electronic signature" to describe a signature with certain characteristics: it is unique to the person using it; it is capable of verification; it is under the sole control of the person using it; it is linked to the data in such a way that if the data are changed, the signature is invalidated, *i.e.* it will not read correctly; and it conforms to regulations made by the Secretary of State.

The UETA drafting meetings have faced similar challenges. The early drafts of the UETA contained a number of presumptions of integrity of the records and their attribution when they appeared with a secure electronic signature.[129] These presumptions and these signatures depended on the parties complying with "security procedures", a term developed in Article 4A of the UCC dealing with electronic funds transfers among banks. The use of appropriate security procedures was said to make the records so trustworthy that the person wishing to rely on them should benefit from a presumption that they had not been altered and that they came from the source identified by the security procedure. This would reverse the common law position that the relying party takes the risk of fraud or forgery.

A number of participants in the UETA meetings argued that such presumptions were not justified by the technology — that is, the technology and in particular its implementation in particular cases

125. Utah Code, s. 46-3.
126. States following the Utah model were Washington, Mississippi and Minnesota. State legislation can be found at http://www.mbc.com/legis/[state name].html.
127. California Government Code, s. 16.5.
128. See footnote 82, *supra*.
129. See for example the August 1997 draft at http://www.law.upenn.edu/library/ulc/uecicta/ect897.htm.

were not as reliable as they were said to be.[130] More important, the practices of key distribution and management (such as identifying properly the person entitled to a key pair, and keeping digital signature private keys private) were too easily compromised and it would be too risky for most people to possess a digital signing mechanism if they would be liable for everything done by it. The situation was contrasted with that of credit card holders, who have a limited liability for the improper use of their card. This limited risk has led to comfort in using the cards, and the credit card industry had benefited from this. It was said that the UETA should not go in the other direction. Article 13 of the Model Law, on which the UETA was based, was itself criticized as unclear, especially when applied to open systems not governed by agreement between the parties.[131]

The early draft UETA also set up a negligence standard. A party that was negligent in handling the private key or other "secure" signing device would be liable to another party that relied in good faith on the signature generated with the device, whether or not the key holder had in fact signed. This was criticized on the ground that the standard of care for electronic signing devices was not known and therefore people would not know how to act reasonably to avoid liability for their devices. By the April 1998 meeting, all presumptions had been removed from the UETA.

The same efforts were seen internationally. UNCITRAL decided, after completing the Model Law, to turn its attention to electronic signatures, no doubt influenced at the time (June 1996) by the apparent success of the Utah statute and some private sector support through the American Bar Association Section of Science and Technology.[132] UNCITRAL has been working for over two years on uniform rules on signatures, which it has called "secure" or "enhanced" but which it defines along similar lines to Illinois. There are intense debates on the legal results to attach to these signatures, and on whether it makes sense to use technology-neutral language when digital signatures are the only ones now known to meet the criteria

130. See in particular notes of the September 1997 meeting at the ETA Forum site, *supra*, footnote 109.

131. A thorough discussion of attribution issues, including those in Article 13 of the Model Law, appears in http://www-personal.monash.edu.au/~bren/thesis/.

132. See *Official Records of the General Assembly (United Nations), Fifty-first session, Supplement No. 17* (A/51/17), paras. 223-224.

for secure signatures (though then only in some implementations).[133] The ability of the "signing" technology to guarantee secure (unaltered) records is also under examination, but this aspect seems unlikely to justify the effort if the signature issues remain unresolved.

However, the favoured status of digital signatures may not be as assured as it has appeared to be. Proponents of competing technologies offer their own products as equivalents.[134] More important, it is increasingly clear that public key cryptography can be used in commerce in many different ways. Some delegates to UNCITRAL advocate an "implementation neutral" law, to operate however the signatures and certificates and document transmission are organized. In addition, some people are criticizing the very trustworthiness of the certification process and the usefulness of a certificate that tells the recipient only the identity of the originator of the message.[135]

These debates are far from over. It should be clear, however, that digital signatures will need a very tightly controlled environment to ensure their reliability or to justify the enhanced legal status that some people want to give them. The Canadian government proposes to set up a Public Key Infrastructure (PKI) to support the use of digital signatures for federal government purposes.[136] In the first phase, only public servants will be issued signing keys, and the government will certify their identities. Later this is expected to extend beyond the government, especially through cross-certification with other public key infrastructures.[137]

Bill C-54 therefore adds to the UECA-type provisions discussed above a number of sections that give legal effect to a "secure electronic signature", defined as "an electronic signature that results

133. Descriptions of the discussions and draft provisions of what are currently being called Uniform Rules on Electronic Signatures can be found at the UNCITRAL web site, http://www.un.or.at/uncitral/english/sessions/wg_ec/index.htm.

134. See for example http://www.penop.com.

135. See for example John D. Gregory, "The Authentication of Digital Legal Records" (1999), 6 The EDI L. Rev. 47.

136. See http://www.cse-cst.gc.ca/cse/english/gov.html for a description and supporting documents from the Communications Security Establishment, and http://www.cio-dpi.gc.ca/pki/pki_index_e.html for the chief information officer's documents.

137. There is obviously a policy difference between saying that the government will use a particular technology and implementing it, on the one hand, and requiring private parties to use particular technology for prescribed purposes among themselves on the other.

from the application of a technology or process prescribed by regulations made under subsection 48(1)". Consultation documents issued in the spring of 1998 by the federal government[138] suggest similar considerations to those in California, Illinois, and UNCITRAL. Signing with a secure electronic signature permits one to certify a public document for purposes of admissibility (s. 36); to seal a document (s. 39); to make a statement under oath (s. 44); to certify the truth of a statement (s. 45); and to witness a signature, if the signer and the witness both use their secure electronic signature (s. 46).

The technical challenges of setting up a valid PKI are well beyond the scope of this article.[139] By introducing Bill C-54, the federal government has declared that it will have met those challenges well enough to justify the enhanced legal status that its product, the secure electronic signature, is accorded in the Act.

2. Licensing Information

Computer software may be protected under a variety of intellectual property regimes. There used to be debates about whether software was subject to copyright, but the courts and the Copyright Act[140] have resolved the question by saying that it is. (Some forms of software have qualified for patent protection in some countries as well.)[141] Intellectual property is a package of rights that is divisible and reproducible. The holder can grant some rights and retain others, or grant some to one person and another set to someone else, or grant some rights for one territory and other rights for another territory. Likewise, the creators of intellectual property often find that they can maximize their economic returns by subdividing rights by time. Rather than transferring it outright, they licence it. This is true of software producers as it is for other forms of such property.

Licences in themselves, when entered into in fully negotiated and voluntary agreements, generally do not present a legal problem; they are a form of contract. However, when the licensed product becomes a standard product available to a mass market, the contract faces novel legal issues. To start with, how does one

138. See http://canada.justice.gc.ca/Consultations/facilt7-en.html.
139. See http://www.pkilaw.com, and the Massachusetts state web site on electronic government, at http://www.magnet.state.ma.us/itd/legal/pki.htm .
140. R.S.C. 1985, c. C-42.
141. Software may contain trade marks and trade secrets. It may, of course, also be subject to contractual restrictions on use and disclosure, as discussed in this section of the article.

tell the potential customer that the transaction available to him or her is a licence, not a sale? A licence is more complicated than a sale: it has potentially more terms, and the terms are less predictable, because of the variety of ways that intellectual property can be divided. Much software is offered in the market on a tangible medium, such as diskettes or CD-ROMs. To what extent does the law of the sale of goods apply to the transfer, and to what extent are licences different?[142]

Some of these issues were discussed in the first section of this article dealing with shrinkwrap and clickwrap licences. In the United States, efforts are being made to create uniform legislation to deal with software and information licensing. Originally these efforts were directed at adding a new Article 2B to the Uniform Commercial Code.[143] Now a simple uniform statute outside the code is proposed.[144] The draft legislation proposes to resolve the general question of the parties' ability to control the use of information by contract. What terms apply to licences in default of agreement (if, for example, a shrinkwrap licence is not enforceable or if it does not cover everything)? Are the parties restricted in what they can agree to in transferring information? May the licensee be restricted in retransferring the property? The statute also expressly validates shrinkwrap licences and sets out procedures for valid clickwrap licences, with still unresolved limits for consumer protection.

In short, the law is being pushed forward to accommodate and to promote on-line commerce. As noted in the jurisdiction discussion earlier,[145] the transfer of property by electronic means makes the licensing issues more urgent, and draft Article 2B also attempts to provide rules on choice of law and jurisdiction to help define the parties' expectations.[146]

142. In the United States, courts have tended to apply Article 2 of the UCC on sales of goods to the transfer, even nominally by licence, of software on hard media like diskettes. See generally Amelia H. Boss, "Developments on the Fringe: Article 2 Revisions, Computer Contracting and Suretyship" (1991), 46 Bus. Law. 1803 and A.H. Boss and J.B. Ritter, "A Legislative Response to the Issues of Software Contracting", [1993] Commercial Law Ann. 27. Outside the tax field, there seems to be little or no Canadian experience on the question.

143. For drafts of proposed Article 2B and the newly named Uniform Computer Information Transactions Act, see http://www.law.upenn.edu/library/ulc/ulc.htm. For more details, see also http://www.2bguide.com.

144. See http://www.nccusl.org/pressrel/2brel.htm, April 7, 1999.

145. See Section II(7).

146. For a detailed discussion of the choice of law and forum clauses in draft Article 2B, see Amelia H. Boss, "The Jurisdiction of Commercial Law: Party Autonomy in Choosing Applicable Law and Forum under Proposed Revisions to the Uniform Commercial Code" (1999), 32 Int'l. Law. 1067.

There seems little appetite in Canada to launch a similar debate. The apparent lack of interest may show that our software producers are not having the same legal problems, or that many of the vendors of software in Canada are Americans more focused on U.S. law, or that people just want to wait and see. This is possibly a prudent course, given the fervour, not to say acrimony, of some of the Article 2B discussions. However, it is hard to imagine our law not being shaped by the results of the Article 2B debate in the medium term, and the contracts that many of us face from U.S.-based or U.S.-influenced licensors will reflect those results even sooner.

3. Consumer Protection

Electronic commerce used to be carried on principally between businesses. Electronic data interchange, using structured data formats and often resting on a trading partner agreement, is for relatively sophisticated players with command of advanced technology. Some people argue that the greatest bulk of e-commerce will continue for a long time to be at the business-to-business level. However, smaller businesses are becoming involved, as the technology allows smaller transactions by less sophisticated people. This results, for example, in the Article 2B discussions dealing with "mass market" licences because a small business licensee has no more significant bargaining power in the face of a large software producer than does a consumer. The distinction between business and consumer is sometimes blurred.

In any event, a great deal of public attention has focused for the past few years on the potential for direct consumer participation in electronic commerce, driven by increasingly user-friendly access points to the Internet like the World Wide Web. Over the past 30 years, most legal systems have developed legislation to protect consumers in commercial transactions, focused on the need for complete information, methods to resist high-pressure sales techniques, and outright bans on some unsavoury practices. The question is whether those protections are also apt for the on-line world.[147]

147. Alberta's Fair Trading Act, S.A. 1998, c. F-1.05, deals among other things with consumer transactions in cyberspace.

The Office of Consumer Affairs of Industry Canada recently commissioned a study of consumer legal issues raised by electronic commerce.[148] It identified a number of issues in need of resolution: contract formation, form requirements, jurisdictional issues, contents of the contract, misrepresentations, conditions and warranties, interpretation of the contract, cooling-off periods, delivery of goods and services, and redress mechanisms. The study admitted that many of them did not have clear answers under present law or present technology, and many of them were matters for provincial rather than federal law. The Uniform Law Conference received an extract of the Industry Canada report at its meeting in the summer of 1998, and it seems an ideal participant in any process to explore possible changes to legislation.

A working group of the federal-provincial-territorial Consumer Measures Committee is working on some of the implications of the report and developing principles for consumer protection laws in the electronic world. Two of the main principles are that consumers should be no less well protected in electronic commerce than they are in other commerce, so equivalent measures should be devised when the old rules cannot work; and that disputes involving consumers should be resolved where the consumer resides.

The OECD resolved at its Ottawa meeting in October 1998 to pursue work on the principles of consumer protection in electronic commerce.[149] In the United States, the Federal Trade Commission is revising its rules on disclosure to consumers to provide for electronic communications.[150]

David Waite discusses these issues in his article[151] and I defer to his expertise and his up-to-date information.

4. Privacy

The more individuals are involved in on-line commerce, the more people will be concerned over how the personal information transmitted over those lines is handled. Computers have wonderful

148. See http://strategis.ic.gc.ca/SSG/ca01031e.html.
149. See http://www.oecd.org/subject/e_commerce/ebooks/ecomm1_4.pdf.
150. See for example http://www.ftc.gov/bcp/rulemaking/elecmedia/index.htm.
151. "Consumer Protection Issues in Internet Commerce", *post*, p. 132.

abilities to process data, and personal data is no exception. Information can be segmented and collated and compared and reassembled and distributed, all to users and for uses far from those contemplated when the information was originally collected. It is also possible to collect information without a person knowing it is being collected, either benignly, to save time in providing better service to the person, or maliciously, to find out things that people would rather not have known.

Canada has few laws governing the collection and use of personal information in the private sector. Consumer reporting agencies, *i.e.*, credit rating businesses, are subject to special rules in many provinces.[152] Four provinces have a statutory tort for the invasion of privacy, though few if any suits are brought on this cause of action.[153] One or two provinces have begun the process of regulating the use of health records, more or less comprehensively.[154] Few of these laws contemplate the kinds of collection, use or disclosure of personal information possible in electronic commerce. Private rights of action may in any event be inadequate to discover and pursue improper data collectors.

Not everyone is persuaded that the threats to personal privacy in electronic commerce need a legislative response. In 1996, the Canadian Standards Association (CSA) adopted a Model Code on the protection of personal information that sets out rules or suggestions for handling personal data.[155] Many businesses have publicly subscribed to the Model Code, and some industrial sectors have developed sectoral codes based on the CSA Model. It is argued that if the public really wants to protect privacy, they will deal with online businesses that promise credibly to protect their data. If the

152. See for example the Consumer Reporting Act, R.S.O. 1990, c. C-33.

153. British Columbia, R.S.B.C. 1996, c. 373, Manitoba, R.S.M. 1987, c. P125, Newfoundland, R.S.N.1990, c. P-22 and Saskatchewan, S.S., c. P24. The Uniform Law Conference adopted a Uniform Privacy Act in 1994, creating a statutory tort after many years of consideration: see Annual Proceedings of the Conference for 1972, 1979, 1985, 1986, 1989, 1990, 1991 and 1994.

154. Manitoba has passed The Personal Health Information Act, S.M. 1997, c. 51. Alberta, Saskatchewan and Ontario have released consultation documents on protecting health care information: see, for example, http://www.gov.on.ca/health/english/pub/legis/phipa/phipa.html.

155. See http://www.csa.ca for a description; the text is available on order. Part of the text is also appended to Bill C-54 as Schedule 1.

desire for protection is exaggerated, then other businesses will continue to thrive. All that is needed is disclosure and education.[156]

This argument runs into at least three objections. First, many consumers, especially those venturing into the big unregulated Internet, may not be sophisticated enough to seek out reliable data protection from businesses that offer it, assuming there are many of them. Second, many techniques for data collection are surreptitious and the danger lies in businesses who will not disclose their techniques and in the consumer not knowing which businesses are unwilling to comply with a voluntary code. Third, the European Union has by its Data Protection Directive required all member countries to enforce privacy standards on their business community.[157] Part of that obligation is to bar the transfer of personal information to any country that does not guarantee similar protection to personal information. This could seriously impede commerce between Europe and Canada, to the disadvantage of Canada, if Canadian standards are judged inadequate. Voluntary adherence, even to a good code, may not satisfy that directive, and in any case requiring every enterprise to prove its compliance before every transfer of data is itself a serious barrier to commerce.

Yielding to these arguments, Quebec in 1994 put privacy rights into the Civil Code of Quebec.[158] The right to privacy had already appeared in the Quebec Charter of Human Rights and Freedoms.[159] In addition, Quebec passed its Act respecting the protection of personal information in the private sector[160] to protect privacy in the private sector, including enforcement mechanisms.

The Uniform Law Conference began work on a Uniform Data Protection Act in 1995, and has considered reports and drafts since that time.[161] The most recent draft was reviewed in August 1998. The conference proposed to legislate compliance with the CSA

156. Several private organizations offer to certify the privacy practices of web sites, among them the (U.S.) Better Business Bureau, at http://www.bbbonline.org and TrustE, http://www.truste.org.

157. See the Directive at http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm.

158. Book 1, Chapter 3.

159. R.S.Q. 1977, c. C-12.

160. S.Q. 1993, c. 17.

161. See the Annual Proceedings of the Uniform Law Conference for 1995 (Appendix M — http://www.law.ualberta.ca/alri/ulc/95pro/e95m.htm), 1996 (Appendix C — http://www.law.ualberta.ca/alri/ulc/96pro/e96c.htm) and 1997. The work has been sidetracked by Bill C-54 and its fallout.

Model Code, since that code was developed through extensive consultation among government and private sector representatives over several years and has obtained wide consensus. The Uniform Act would also have contained enforcement provisions, possibly relying on the existing machinery for enforcing public sector privacy rules, which most provinces and the federal government have had in place for some time.

In October 1998 the federal government introduced the Personal Information Protection and Electronic Documents Act, Bill C-54,[162] other parts of which were discussed previously in the section on statutory barriers to electronic commerce. The federal bill is much like the proposed Uniform Act; federal officials had led the uniform law project up to this time. It legislates compliance with the CSA Code and provides for enforcement. It deals with commercial uses of information and exempts personal data collection not used for commercial purposes. It also exempts "any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose".[163] The bill does not expressly deal with collection of personal information by not-for-profit organizations for fundraising, except to the extent that this would be collecting or using it interprovincially or internationally.

The bill is intended to apply to federally regulated businesses and to personal information transmitted across provincial borders or the national border.[164] It also purports to extend to all collection, use and disclosure of personal information for commercial purposes three years after its coming into force.[165] However, any province that has enacted similar legislation would be exempted from the federal scheme, at least to the extent of the common coverage. It is possible that the federal government is concerned to ensure provincial compliance with the standards of the European Data Protection Directive mentioned earlier. The constitutional validity of this extension is not clear.

5. Dispute Resolution

Electronic commerce poses several difficulties to the traditional systems for resolving commercial disputes. One is the jurisdictional problem: where is a person located in electronic commerce?

162. See footnote 33, *supra*.
163. Bill C-54, para. 4(2)(c).
164. Bill C-54, s. 4.
165. Bill C-54, s. 30.

Another is the scale of electronic commerce, especially for consumer transactions: is there enough money in the deal to justify proceedings? Another is the speed and informality that are among the main benefits of electronic commerce. They can best be maintained if disputes can be handled in the same way.

These difficulties have led to considerable interest in alternative dispute resolution (ADR). Alternative dispute resolution is a broad umbrella covering many flexible techniques for resolving disputes. Its scope is beyond the mandate of this article. Discussions of how to apply ADR on-line are just beginning.[166] One should note, however, the beginnings of on-line dispute services, including at least one located in Canada at the Université de Montréal.[167] Industry Canada recently commissioned a study of dispute avoidance and resolution in electronic commerce that catalogued the main initiatives in this field. A conference of the main dispute resolution on-line providers was held in Montreal in June 1998, and a web site is available for further information.[168]

6. Summary

All of these "promotional" developments aim to help many participants in electronic commerce feel more comfortable with investing money in the Internet. They therefore encourage and promote further expansion of the potential for e-commerce. Some of these initiatives are more promising, or promise more immediate returns, than others. Some of them are pioneering in little known areas. As noted earlier, a good deal of the potential territory of electronic commerce is already explored and is already host to much activity.

V. CONCLUSION

Electronic commerce raises legal issues that have struck people as novel, thus requiring novel solutions. On further examination, many of them have turned out to be resoluble under traditional

166. See Christine Hart, "Online Dispute Resolution and Avoidance in Electronic Commerce" on the ULCC web site, http://www.law.ualberta.ca/alri/ulc/eindex.htm.
167. See http://www.cybertribunal.org.
168. *Ibid.*

legal analysis. Others are subject to fairly limited statutory fixes.[169] Most do not require re-examination of the basic principles of fairness and efficiency that the existing rules are intended to promote. It is clear, however, that legal solutions should be harmonized within a market, and the global market of electronic commerce requires large-scale efforts at harmonization. For this reason Canada has hosted the OECD ministerial meeting and has been an enthusiastic participant at the UNCITRAL working group on electronic commerce. The Uniform Law Conference has had no difficulty persuading its bureaucratic masters of the importance of the electronic commerce project. The priority in the Uniform Law Conference is the same as that of UNCITRAL: first remove the barriers, then look to promotion.

Some of the promotion efforts may be premature or oversold. Some, like privacy rights and dispute resolution, seem destined for expansion. However, the market and the need for legal certainty are evolving quickly. The challenge is to keep one's perspective and not indulge in fast-track law reform that ends up irrelevant to where the market is going, or worse, that forces the market into inefficient or uncompetitive paths. However, market preferences must be balanced against consumer interests and public interests. The examples in this article suggest that such interests can be accommodated without undue harm to innovation and competition. No harmonization effort will prevent the rise of "data havens" where rules of the world community may not be respected. Nevertheless, participants in electronic commerce will find many advantages in dealing in places and with businesses that abide by known rules. A combination of voluntary preference and focused government action will create a rule of law even in cyberspace, at least in the parts where most people choose to go.

169. As markets and technology evolve, the immediate task for particular fields of law may shift from private accommodation to statute or vice versa. The categories of analysis used in this article are not impermeable or permanent.