

The Law Goes Electronic

John D. Gregory*

[2009] Annual Review of Civil Litigation 127

I. INTRODUCTION

II. THE NATURE OF ELECTRONIC DOCUMENTS

- 1. The Vulnerability of Bits and Bytes**
- 2. Security**
- 3. Standards**

III. REMOVING BARRIERS IN EXISTING LAW

- 1. Barriers in Existing Law**
- 2. Principles of Legislation**
 - a. Media neutrality**
 - b. Technological neutrality**
 - c. Minimalism**
 - d. Consent**
 - e. Equivalence of risk**
- 3. Examples of Enabling Legislation**
 - a. Writing**
 - b. Signature**
 - c. Originality**
 - d. Evidence**
 - e. Record retention**
- 4. Canadian Legislation**
 - a. Uniform legislation**
 - b. Implementing the Uniform Act**
 - c. Federal legislation**
 - d. Quebec legislation**

IV. ELECTRONIC COMMERCE

- 1. Authentication and Signatures**
- 2. Electronic Contracts**
- 3. Consumer Protection**

* General Counsel, Justice Policy Development Branch, Ministry of the Attorney General (Ontario). The views in this article are not necessarily those of the Ministry. All Internet addresses were valid as of September 10, 2011.

V. ELECTRONIC GOVERNMENT

- 1. Government as user of electronic communications**
 - a. Incoming documents**
 - b. Outgoing documents**
- 2. Governing electronically**
 - a. Dispute resolution**
 - b. Regulation**

VI. LITIGATION ISSUES

- 1. Electronic Communications**
 - a. Service**
 - b. Filing**
 - c. Trials**
- 2. Electronic Discovery**
 - a. E-Discovery in general**
 - b. E-Discovery and privacy**
- 3. Electronic Evidence**
 - a. Admissibility in general**
 - b. The best evidence rule**
 - c. Metadata**
 - d. Some special cases**
 - e. Weight of the evidence**
- 4. Electronic Practice of Law**

VII. EMERGING ISSUES

- 1. Web 2.0**
- 2. User-generated content**
- 3. Virtual worlds**

VIII. CONCLUSION

I. INTRODUCTION

Everybody knows that computers are everywhere. Also, they talk to each other, across the office or around the world instantaneously. Texts, pictures, movies, conversations: everything is electronic, or can be. Our society, our commerce, and our government have been profoundly affected, and the developments continue ever more quickly.

Society, commerce and government in Canada are all subject to the rule of law. The law expresses the desired relationships among us and sets limits to them. Normally the law trails developments; it rarely leads them. The speed with which electronic records and communications have pervaded our lives has risked leaving the law further behind than usual, threatening its capacity to guide, validate and control the areas touched by them – which is just about everything.

Considerable efforts have been made to keep the law up to date, either by thinking about its traditional concepts in new ways or by changing the law itself. This article reviews some of the major themes of legal thinking and law reform designed to reflect the electronic age.

We will start by considering the nature of electronic records and communications: what is the problem, anyway? We then turn to the legal first response: removing the barriers to innovation posed by the traditional rules of law. From there, we look at some of the ways in which electronics affect typical legal activities, such as trying to know who and what one is dealing with, where things are being done, and how one controls such things in an immaterial environment. Next we review some of the areas where civil litigation is particularly affected, notably including discovery, evidence and judicial processes. We finish with a brief look at the directions of innovation in the technology and how the law may evolve to keep up.

The article will deal very little with substantive areas of law, even though some are extensively affected by electronic communications; privacy¹ and intellectual property² are two important examples.

THE NATURE OF ELECTRONIC DOCUMENTS

1. Vulnerability of Bits and Bytes

Why do people care about electronic documents?³ What is it about them that causes concerns about the applicability of the usual rules of law? While it is true that some of the concerns diminish with closer analysis, electronic documents are different in several ways from those on paper.⁴

1 Thorough examinations of privacy issues can be found on the websites of Canadian privacy commissioners. Two rich sources of discussion are the sites of the Information and Privacy Commissioner of Ontario, online: <http://www.ipc.on.ca>, and of the Privacy Commissioner of Canada, online: <http://www.privcom.gc.ca>.

2 See for example the new Intellectual Property Law and Technology Program at Osgoode Hall Law School, York University, known as IPOsgoode, online: <http://www.iposgoode.ca/ip-osgoode-program-for-intellectual-property-law-technology>.

3 This article will use “electronic document” and “electronic record” interchangeably. Some statutes use one expression, some another. Ontario is not consistent internally. The *Evidence Act*, R.S.O. 1990 c. E.5, s. 34.1, speaks of electronic records. The *Electronic Commerce Act, 2000*, S.O. 2000 c. 17, speaks of electronic documents. The latter phrase is easier to translate into French, and has made some legislative headway in Canada for that reason.

4 These questions are examined in more detail in J.D. Gregory, “Authentication Rules and Electronic Records”, (2002), 81 *Canadian Bar Review* 529.

Electronic documents are a set of instructions about electric current, to turn the current on or off. A bit is a yes-or-no (one or zero) instruction about current flow. A byte is a combination of seven or eight bits. There are enough possible combinations in a byte to permit the designation of the characters of most alphabets and numbers from zero to nine. Electronic documents commonly show the results of these electronic instructions as words or numbers on a screen, or printed out on paper. Though they “look like” writing, several concerns have prevented their general acceptance as writing.

First, the storage of electronic instructions may be uncertain. The storage medium, whether a computer's hard drive, a removable medium like a compact disc or magnetic tape, may not be stable. Some data may be lost over time, even without human intervention. Data may also be lost in transmission to other media. The software and hardware needed to retrieve the data may evolve, and keeping up with that evolution may affect the integrity of the data.

Second, retrieving the data can be problematic. Sometimes data are created in one format (such as Microsoft Word) and retrieved in another (such as OpenOffice). Not all the instructions are compatible among all systems, so content or format may be affected even in apparently routine operations.

Third, as electronic documents are just a collection of instructions, they are susceptible to having the instructions changed by anyone with the right software and access to the document. Once they have been changed, the resulting document may show no sign of the change. A copy of the instructions may be perfect, not distinguishable in any manner from the version first created. Further, evidence of origin – like a signature – is itself electronic and thus subject to the same undetectable alterations as the signed text.

These factors make it harder for people to evaluate the reliability of electronic documents. While words and numbers on paper are vulnerable in many ways, literate society has centuries of experience in deciding what is reliable and in using means to reinforce reliability when it is important. We have been dealing with electronic documents for much less time, and many people are thus uncomfortable estimating and reinforcing their reliability.

2. Security

The security of the electronic document is thus close to the surface of almost any discussion of the legal status of electronic communications, in a way that it is not for its paper equivalent. How do we know what we are dealing with, and where it came from? Information security can be a very technical subject,⁵ but here are a few of the suggestions that are frequently made:

- Check the integrity of the storage process, at least by sampling, when paper records are transferred to electronic format, or even in communicating electronic records from one place to another.
- Use trustworthy processes, which involves knowing the capacity of the technology and the levels of risk involved in any particular record, communication or transaction.

5 For a brief summary of techniques for protecting one's system, see R. Jueneman, “What You Should Do to Combat Information Security Threats”, online: <http://www.jueneman.com/recommendations.html>. For a legal overview, see T. Smedinghoff, *Information Security Law: The Emerging Standard for Corporate Compliance*, (IT Governance Ltd, 2008). Security for lawyers in their practices is discussed below in section VI:4.

- Control access to the means of creating electronic records, including physical and electronic access.
- Use trustworthy people, since it is not just strangers who may be the source of problems.
- Use secure communications methods; the more insecure the data are, the more secure the communications should be, and vice versa.
- Use a trusted third party to help support reliability when relevant facts are not otherwise ascertainable.

These methods of making one's own e-documents reliable can obviously be turned into questions one asks of such documents that one is invited to rely on. One is impelled to a kind of 'threat-risk analysis', or a cost-benefit analysis: do the likelihood of causes of unreliability, the extent of their impact on the documents, and the gravity of the impact on the legal relations supported by the documents, outweigh the benefit of relying on them? Different people will answer this question differently. The answer will also vary with the nature of the documents, the value of the transaction, and the history of dealings between the parties to the communications.

How much reliability is enough is ultimately a business question, not a technical question, though familiarity with the applicable technology will help answer it. "Business" in this context includes "legal". Not only do the legal risks vary in different situations, but the legal purpose of relying on the document will affect the judgment. Is it a document to be admitted into evidence, a contract on which future commerce will be conducted, or a certificate of a public authority? We will see later in this article how the law has dealt with these different effects in the electronic age.⁶

3. Standards

While it is legitimate to question the reliability of any electronic document or communications, it is also very time-consuming. A number of shortcuts exist. The main one is the existence of technical standards, both proprietary and public.

As e-documents are sets of instructions about the flow of electric current, if the documents are to be widely understood, the instructions have to be shared. This is done by using common software to create and to read the documents. Hardware too meets common standards, in order to respond correctly to the software. This is true for any electronic record, whether stored or communicated. Think of using Microsoft Word to read a document created in WordPerfect, or even different versions of Word. If the standards are slightly different, the features of the text may differ too. The sharing of the standard may be more or less complete.

The Internet is essentially a set of shared standards for creating and referring to e-records so that all computers can understand them. Without the Internet Protocol, very little e-communication would happen. The myriad different applications for e-communications show that the standards are not restrictive, just compulsory.⁷

6 The International Telecommunications Union (ITU) has recently created the International Multilateral Partnership Against Cyber Threats (IMPACT) to provide resources to all countries on combating threats to IT security. More detail is online: <http://www.impact-alliance.org>. See also the [Organization for Economic Cooperation and Development \(OECD\), Computer Viruses and other Malicious Software: A Threat to the Internet Economy](#), (OECD, 2009), online: http://www.oecd.org/document/16/0,3343,en_2649_34223_42276816_1_1_1_37441.00.html.

7 There is a fascinating debate not relevant to this article about how much "intelligence" should be built into the system and how much left to the applications that run on it.

While these standards are generally designed to facilitate communications, the way they go about it may have implications for policy, either legal or political.⁸ For example, the way that computers break down instructions into packets and route them individually through whatever channel is most readily available tends to make messages hard to intercept during transmission. This affects law enforcement practices. The way Internet Protocol addresses are distributed and attached to the packets may make the originator of a message more or less difficult to identify.⁹

The average lawyer faced with the average electronic document is unlikely to have to go behind the technical standards that make the electronic format possible. It is useful to recall that the standards can have such an impact, however, for the occasional situation where just such an examination will repay the effort.¹⁰

III. REMOVING BARRIERS IN EXISTING LAW

1. Barriers in Existing Law

The first challenge that faces the lawyer dealing with electronic communications is whether their use has any legal effect. The main reason this question arises is that most of the law predates such communications. Many legal rules were formulated in language that assumes a paper support for the information involved. Thus we find rules that notices be in writing, or that documents be signed, or that original records be produced.

It is hard to tell if the legislators or the courts or the private lawyers who made these rules really wanted paper and would have refused to allow an electronic equivalent if given the choice. It can also be difficult to know whether electronic communications do satisfy these requirements anyway. Is an electronic document a form of writing, when it appears on a screen as traditional letters and looks like a document of similar import on paper? Is a name at the bottom of a document or form in the usual place for a signature, possibly looking like a handwritten signature or preceded with the word “signed”, a signature? Does the term “original” have a meaning when applied to an electronic document, and if so, what is it, when that document may be at the same time, and composed of exactly the same instructions as to the bits and bytes that compose it, in one or more computer hard drives, an email server, and several varieties of movable media like compact disks and USB drives?

One leading Canadian expert on the law of information technology has suggested that the law has four techniques (“skill sets”) for dealing with these questions: contract, technology, common law and legislation.¹¹ Contract is the first recourse, certainly for the transactional lawyer. One can simply

8 This observation was developed by L. Lessig, *Code and other laws of Cyberspace* (1999)(now second edition, *Codev2*, online: <http://codev2.cc>; and J. Reidenberg, “Lex Informatica: The Formulation of Information Policy Rules through Technology”, (1998), 76 Texas L.R. 553.

9 The redesign of the basic Internet Protocol to multiply its capacity to serve different addresses, and thus to accommodate the explosion of users, also involved greater traceability of the computers with those addresses. Privacy advocates expressed concern with this feature, and arguments ensued about whether it was inherent or avoidable. See the European Commission, *Discussion Document from the European Commission Ipv6 Task Force to Article 29 Data Protection Working Group*, (February 2003) online: http://www.eu.ipv6tf.org/PublicDocuments/Article29_v1_2.pdf

10 See the discussion of metadata in the Evidence discussion below, text accompanying note 255.

11 G. Takach, *Computer Law*, 2nd Edition, Irwin Law, 2003, p. 3 and 690 – 700.

specify that communications may be electronic, or one may spell out that electronic documents satisfy the legal form requirements of writing, signature and so on. While this is very helpful, it is subject to many limits. Not all legal relationships are subject to contract at all. It is not clear that private arrangements can override mandatory rules requiring paper – if they are mandatory.

Technology can answer questions about the reliability of e-documents but on its own is inadequate to ensure that such documents meet existing form requirements.

The common law does provide much flexibility. Canadian courts have decided that click-through contracts can be binding on the parties to them,¹² that a faxed proxy was satisfactorily signed,¹³ that corporate notices could be sent to shareholders by email,¹⁴ that an arbitration clause on a website was enforceable,¹⁵ and even that an Internet service provider could rely on the rules of “netiquette” to terminate service of a spamming customer.¹⁶

The problem with the common law, though, is that it develops only as cases arise, and only on issues that parties choose to litigate. Given the wide, even universal, adoption of e-communications, too many questions were left unanswered by the gradual evolution of the common law. Also, not all judicial decisions are equally satisfactory.¹⁷

As a result, many jurisdictions including Canada have turned to legislation to ensure that e-communications could be legally valid in the face of existing legal form requirements.

2. Principles of Legislation

The legislation in most of Canada and in many of the countries with which it trades is based on similar principles, worked out in international and national discussions over a decade or more.¹⁸

(a) Media neutrality

The law should work the same regardless of the medium of communication used. Put another way, the media chosen to convey information with legal effect should be interchangeable without loss of effect. There should not be two (or more) sets of law, one for communications on paper and another parallel

12 *Rudder v Microsoft Corp.* (1999), 2 C.P.R. (4th) 474 (ON SC)

13 *Beatty v First Exploration Fund* (1988) 25 B.C.L.R.2d.377.

14 *Re. Newbridge Networks Inc.*, (2000), 48 O.R. (3d) 47 (ON SC)

15 *Dell Computers Corp. v Union des consommateurs*, (2007), 2 S.C.R. 801. See also *Kanitz v Rogers Cable Inc.* (2002), 58 O.R. (3d) 299 (ON SC).

16 *1267623 Ontario Inc. v Nexx Online Inc.* (1999), 45 O.R. (3d) 40 (ON SC)

17 The decision in *Kanitz*, above note 15, that an arbitration clause could be added to a contract on paper by posting a notice on a website led directly to provisions in Ontario's *Consumer Protection Act, 2002*, S.O. 2002 c.30. Sched. A, s .7, reversing it. V. Gautrais, “Le vouloir électronique selon l'affaire Dell Computer: dommage!” (2007), 37 *Revue générale du droit*, online: <http://www.gautrais.com/IMG/pdf/200702GautraisEpreuve1.pdf> . In *Department of Transportation v Norris*, the Georgia Court of Appeals held that a fax could not be certified mail because “the transmission of beeps and chirps along a telephone line is not writing, as that term is customarily used.”. 474 S.E.2d 216, 217 (1996)

18 One of the early documents calling for general law reform to deal with electronic documents in commercial settings was by the United Nations Commission on International Trade Law (UNCITRAL) in 1985. Report of the Secretary-General, *Legal Value of Electronic Records*, United Nations Document A/CN.9/265, online via the documents for the 1985 meeting of the Commission: <http://www.uncitral.org/uncitral/en/commission/sessions/18th.html>.

but distinct for electronic communications. Legislation has thus set about to say how e-documents can meet the general standards of the law, rather than creating new standards for the electronic world.

(b) Technological neutrality

The law should not require a particular technology or a particular solution to the problems of making e-communications legally effective. Several reasons impel this principle:¹⁹

- Technologies change quickly. By the time legislators can decree a particular technology to be effective, a better one may have appeared, or flaws may have been discovered in the one selected.
- The uses for technology are varied. The right technology for one purpose may not be right for another. Legal prescriptions could be too rigid to permit innovative uses of technology.
- The market for technology to serve various purposes, including legal purposes, is competitive. It is not up to the politicians to “legislate market winners”.²⁰

As a consequence, most Canadian legislation has been careful to use language that allows lawyers and their clients their choice of solution to the technical and legal challenges of electronic documents.

(c) Minimalism

Another characteristic of most Canadian legislation is that it does not give any more detail than needed to remove the barrier of the form requirement it is aimed at. Again, it is important not to tie the hands of innovators by too much detail, even generic. Further, a proper understanding of technological or legal challenges in this field often shows that they are fairly narrow. The history of law reform in this field tends to run from complex proposals to simple solutions, as people work out that existing laws can deal with many of the apparent problems, or that a targeted resolution of one problem can clear the path for several related issues to become clear on their own.

(d) Consent

The other guiding principle of our legislation is that it does not require anyone to use or to accept information in electronic form. The intent is to remove barriers for those who wish to use the electronic route, not to compel the unwilling to go where they are fearful. So the statutes require consent of the parties to the communications.

Not only is this a proper social principle, it is also a key element in secure electronic communications. No single level of security will suit all purposes. Everyone has to decide what level of risk is appropriate for the purpose of any particular electronic communication. If an overly risky technology is proposed, the consent principle allows the risk-averse person to say No. The ability to say No is the ability to say Yes, if ... the security is adequate in the eyes of the party affected.

19 For a concise but fuller discussion, see J. D. Gregory, “Technology Neutrality and the Canadian Uniform Acts”, 4th International Conference on Law via the Internet, 2002, online: <http://informationjuridique.ca/docs/conf/2002/gregory.pdf>.

20 B. Biddle, “Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace”, 34 San Diego Law Review 1225 (1997), online: <http://members.cox.net/biddle/LMW.htm>.

This does put some responsibility on parties to e-communications to be able to evaluate the risks and the security solutions to them. Just because the law permits such communications does not mean that they are always prudent. This is no different from many other areas of the law. The law does not attempt to prohibit all human activities, or even commercial activities, that present risks to the participants. The novelty of e-communications does not change that approach.²¹

(e) Equivalence of Risk

The final principle of facilitating legislation is that electronic documents do not need to be any more reliable than their paper counterparts. Yes, electronic documents can be deleted at the touch of a key.²² So too can paper documents be burned, torn or otherwise disposed of in a matter of seconds. Yes, some forms of electronic signature are questionably linked to their originators. But forgery of signatures is a known problem with ink on paper too, and detecting a forgery a matter of as much art as science.

As noted earlier, in practice our society has had several centuries of general literacy to evaluate the risks of paper records and to develop methods of dealing appropriately with different risk levels and risk tolerances. We have had decades at most to learn to do the same with electronic records. The techniques are not yet second nature to business people, much less to consumers. This difference is one of the main motivations for the call for legislation that does not meet the other principles above. The legislatures in Canada have resisted this call, in the perspective that less restrictive enabling legislation will permit a better development of e-communications, and the net benefit of innovation and widespread adoption of these communications will outweigh the risks of bad judgments about security.²³

3. Examples of Enabling Legislation

The international source of most legislation to remove barriers to the legally effective use of electronic communications is the United Nations Model Law on Electronic Commerce, adopted in 1996.²⁴ The principles just discussed evolved through discussions in the preparation of the Model Law, which therefore reflects them directly.

The UN Model Law rests on the concept of “fundamental equivalence”. When one encounters a rule of law that requires information to be in a particular form, such as in writing, one asks what policy purpose that requirement serves. One then works to find a rule that allows information in electronic form to achieve the same purpose.

21 This does not mean that particular vulnerabilities are not addressed. Just as general commercial rules are often softened when they are applied to consumers, so areas perceived to present special risks are sometimes given special treatment in the laws removing barriers to e-communications. See the discussion below, text accompanying note 46, of exceptions to the general permission to use electronic communications with legal effect, to protect consumers, accommodate particular security needs, and so on.

22 Actually it is difficult to destroy an electronic record thoroughly. Those who really want to accomplish it are often advised that they should destroy the hard drive on which it is stored. See Information and Privacy Commission of Ontario, “Secure Destruction of Personal Information”, 2005, online: http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf.

23 A.Boss, “Searching for Security in the Law of Electronic Commerce”, 23 Nova Law Review (1999) 585. Recall as well the practical security tips above, text following note 5.

24 United Nations Model Law on Electronic Commerce with Guide to Enactment, UN Document A/RES/51/162 (1997), online: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf, referred to here as MLEC.

The alternative is to simply define the electronic record as being in the required form, such as defining an electronic record to be in writing. Besides being contrary to one's observations in some cases, this also can overlook or downplay the risks of the electronic medium, of the kinds noted at the outset of this discussion.

The rules of the Model Law have more recently been restated in the UN Convention on the use of Electronic Communications in International Contracts of 2005, known as the E-Communications Convention.²⁵ The following examples of the United Nations legislative solutions are taken from both documents.

(a) Writing

The Model Law and the Convention provide that where the law requires information in writing, an electronic document²⁶ satisfies that requirement if it is accessible so as to be usable for subsequent reference.²⁷ Put another way, the Model Law's formulation serves the function of memory. Putting something in writing is a way of ensuring that the information is available later, and also available to be shared, that is, referred to by others.

One will note that the Model Law does not require any particular durability of the electronic record. This demonstrates an aspect of the simplicity or minimalism principle referred to above. The notion of writing contains some implication of durability, but no obligation that something be available for any specific length of time. Information may be in writing now, but destroyed tomorrow. A requirement to keep information for a length of time is a record retention rule, which is dealt with separately in the Model Law.

(b) Signature

The Model Law says that a rule of law requiring the signature of a person is met electronically if a method is used to identify the signer and indicate his or her approval of the information, and if the method used is as reliable as appropriate in the circumstances.²⁸ The circumstances can include any agreement among the users of the signed document about the signing method. In this formulation, "approval" is taken to mean only that the signer has agreed to be linked to the signed information, and not necessarily that the information is a contract binding on the signer.²⁹

The Convention modified the reliability test for electronic signatures. It provides that information is

25 General Assembly resolution 60/21 of 23 November 2005 (UN document A/RS/60/21, 9 December 2005), Annex, online: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html. Footnoted here as ECC. A very detailed review of the ECC is found in A.H.Boss and W. Kilian, *The United Nations Convention on the Use of Electronic Communications in International Contracts: An In-Depth Guide and Sourcebook*, (Wolters Kluwer, 2008).

26 The Model Law calls electronic documents "data messages". The ECC refers to an electronic communication.

27 Model Law, article 6(1), ECC article 9(2). The Model Law acknowledges that 'requirements' may also take the form of rules that attach consequences to information that is not in writing, rather than directly making writing mandatory. Nothing in the present discussion turns on this distinction.

28 Model Law (1), ECC article 9(3).

29 See for example the Guide to Enactment of the UN Model Law on Electronic Signatures, above, fn 24, paragraphs 29 and 73.

also appropriately signed electronically if the method is proved in fact to have identified the signer and indicated the signer's intention in respect of the information in the signed document, either by itself or together with other evidence.³⁰

Without this alternative, there was a risk that the reliability test could become a trap for the unwary, a way for someone to avoid an obligation that everyone knew he or she or it had undertaken, simply by arguing that the signature method was objectively too unreliable for the transaction in which it was used, regardless of the agreement of the parties or their knowledge of or ability to prove the facts.³¹ In addition, there is no similar reliability test of handwritten signatures, though there are many ways of signing something, with varying degrees of reliability.³² Recall the principle that electronic information should not need to be more reliable than its paper equivalent, in order to have the same legal effect.

(c) Originality

Where the law requires that information be presented in the form of an original document, the Model Law and the Convention provide that an electronic document satisfies that requirement if the information presents sufficient guarantees of integrity. This means that there are assurances reasonable in the circumstances that the information has not been altered from the time of first creation in final form³³ to the time it is presented or evaluated as an original.³⁴

In short, the UN documents have taken the function of requiring an original to be to aid in ensuring the integrity of the information. On paper, it is harder to alter an original document undetectably than it is a copy. However, the concept of originality is hard to apply to an electronic document, as we have seen earlier. So some other method of demonstrating integrity will have to be found. The UN documents do not say what they must be.

If the purpose of an originality requirement is something else – such as to demonstrate the source of a document, for example, as a public document – then it may be that the UN rules will not work. The Model Law allows implementing countries to exclude particular types of information from its rules. The Convention does not give a right to individual exceptions but does exclude some kinds of transactions and documents from its scope.³⁵

(d) Evidence

The Model Law provides that evidence shall not be denied admissibility merely because it is in

30 ECC article 9(3)(b)(ii).

31 A fuller discussion of this point appears in the author's letter to Singapore's Attorney General's Chambers in the context of a review of that country's Electronic Transactions Act. See J. D. Gregory, "Must e-signatures be reliable?", online: http://www.euclid.ca/reliability_sigs.pdf.

32 Some methods of handwritten signatures are plain signing, signing with initials on every page, signing before a witness, signing before a notary, signing with a personal seal, signing with a bank certificate of signature or of office, and so on.

33 In other words, not a draft of the document to be presented as an original.

34 MLEC article 8, ECC article 9(4,5).

35 Notably it excludes consumer transactions, some communications of regulated financial institutions, and negotiable instruments. ECC article 2. It also allows parties to transactions to vary or derogate from any of its provisions. ECC article 3.

electronic form. It goes on to say that if the electronic record is not an original, it should be admitted if it is the best evidence available.³⁶ This provision was not picked up in Canadian implementing legislation,³⁷ in part because the Uniform Electronic Evidence Act was already in place when the uniform statute on the Model Law was being developed,³⁸ and in part because the requirement for the electronic record to be the best evidence risked making it inadmissible if a paper equivalent was available, since some courts might consider paper to be generally more reliable than electronic information. This was considered unduly restrictive of people's choice to keep information in whatever medium they chose.³⁹

(e) Record retention

The Model Law provides that a rule requiring retention of records can be satisfied by electronic information if the information has the appropriate integrity (as with originals) and is accessible to the people to whom the law requires it to be accessible, for the full period required by law.⁴⁰ This rule applies whether the information was originally on paper but converted to or saved in electronic form, or whether the information was first created electronically. The information is also to include metadata where available, that is, information about the time of its creation or delivery.

4. Canadian legislation

We will now look briefly at how these principles, as reflected in the United Nations Model Law, have been implemented in Canada.⁴¹ As of the spring of 2009, no action has been taken in response to the Convention.⁴²

(a) Uniform legislation

The main legal text to implement the Model Law is the Uniform Electronic Commerce Act (UECA), adopted by the Uniform Law Conference of Canada in 1999.⁴³ The UECA is quite close to the Model Law, except in its treatment of signatures. There, it simply says that where the law requires a signature, an electronic signature satisfies the requirement.⁴⁴ There is no reliability test.

The thinking of the Conference was that neither the common law nor the civil law requires signatures to be in a particular form. Thus an electronic signature is probably valid even without special

36 MLEC article 9. The ECC does not deal with evidence.

37 See the discussion of this legislation in the next section, TAN 43.

38 [1998] Proceedings of the Uniform Law Conference of Canada 164, online: <http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2>.

39 See the discussion of electronic evidence, including the best evidence rule, below at TAN 236.

40 MLEC article 10. The ECC does not deal with record retention.

41 For a more detailed discussion, see J. D. Gregory, "Canadian Electronic Commerce Legislation", (2002), 17 Banking & Finance Law Review 277, online: <http://www.euclid.ca/bflr2002.pdf>.

42 The relation of the Convention to Canadian law was considered in the summer of 2008 by the Uniform Law Conference of Canada. The papers and presentations are found in the Civil Section Documents of the Proceedings of the 2008 meeting, online at: <http://www.ulcc.ca/en/poam2>.

43 1999 Proceedings of the Uniform Law Conference of Canada 380, online: <http://www.ulcc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia>.

44 UECA s. 11.

legislative support.⁴⁵ The UECA does allow for regulations spelling out reliability rules for particular signatures, if desired by an enacting jurisdiction.

The UECA expressly does not apply to some kinds of documents or transactions, notably many real property transactions, negotiable instruments, wills and personal powers of attorney, and a few others.⁴⁶ Some of these were thought to require more security than the minimalist rules of the UECA provided, especially for documents likely to be created by people without technical expertise or legal advice.

The UECA added some features to the Model Law as well, notably a provision for human error in a transaction with a computer, that are beyond the scope of this article.⁴⁷

(b) Implementing the Uniform Act

The UECA has been implemented in all the common law provinces and in Yukon and Nunavut.⁴⁸ There are minor variations, starting with the name. Since the Act is not restricted to commercial matters, some provinces have called their legislation the *Electronic Transactions Act*,⁴⁹ and Saskatchewan chose the *Electronic Information and Documents Act*.⁵⁰ Manitoba has not proclaimed the part of its Act dealing with writing and signatures.⁵¹ Prince Edward Island has a non-uniform description of signatures, for reasons not disclosed in the legislative debates or other documentation.⁵² New Brunswick did not choose to legislate any of the exceptions to coverage of the UECA.⁵³

None of these variances is reflected in case law or appears to have made any difference to the legal effect of electronic communications in Canada. For that matter, there are almost no cases under any of the e-communications legislation in the seven or eight years since most of it was adopted. One can speculate whether this means that the legal challenges for which it was adopted were exaggerated, or that the legislative solutions were so appropriate that no one is impelled to litigate about them.⁵⁴

(c) Federal legislation

The government of Canada adopted in 2000 the *Personal Information Protection and Electronic Documents Act*.⁵⁵ Part 2 of PIPEDA deals with electronic documents. Though it was inspired by the

45 The Law Commission in England arrived at the same conclusion in 2001: *Electronic Commerce: Formal Requirements in Commercial Transactions: Advice from the Law Commission*, esp. para. 3.39, 3.42, online: http://www.justice.gov.uk/lawcommission/docs/Electronic_Commerce_Advice_Paper.pdf.

46 UECA s. 2.

47 Some of these are discussed below at TAN 76.

48 A chart showing implementation across the country, including the federal and Quebec statutes, is available on the Uniform Law Conference of Canada web site, online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4b>.

49 British Columbia (S.B.C. 2001 c.10); Alberta, (S.A. 2001 c.E-6.5) and New Brunswick (S.N.B. c. E-5.5).

50 S.S. 2000 c.E-7.22.

51 *Electronic Commerce and Information Act*, C.C.S.M. c. E55, part 2, ss. 8 – 18, “Using Electronic Means under Designated Laws”.

52 *Electronic Commerce Act*, S.P.E.I. 2001 c. 31, s. 1(1)(b). Hansard, April 10, 2001, p. 1093-1095.

53 *Electronic Transactions Act*, S.N.B. c. E-5.5. The Act left all exceptions for the regulations. See regulation N.B. Reg. 2002-24, which excludes six provincial statutes from the Act.

54 There was not much litigation about e-communications before the UECA either. It has been suggested that parties to e-communications often have an ongoing relationship that they are more inclined to work to repair than to sue about when they have technical problems of communication.

55 S.C. 2000 c. 5, known popularly as PIPEDA. This statute is quoted more often for Part 1 on private sector privacy rules

version of UECA current when it was drafted, the approach is fundamentally different in two respects. First, it applies only on an opt-in basis. In other words, it applies only to rules of law in federal statutes and regulations that have been expressly designated for that purpose in regulations made under the Act. Only one Act and one regulation have been designated in the nine years since it came into force.⁵⁶ On the other hand, several statutes have been enacted with their own provisions about electronic records.

The second big difference is that the federal Act requires that many functions of a signature must be carried out by a “secure electronic signature”.⁵⁷ The broad outlines of this signature are in the Act,⁵⁸ with the details left to regulations.⁵⁹ The essential point is that the secure electronic signature is not technology neutral. Only digital signatures created under the Government of Canada's Public Key Infrastructure (PKI) qualify.⁶⁰ One may assume that the federal government decided that the risks of electronic signatures were too great to leave the technological choices in the hands of the users. Some of the uses are clearly highly sensitive, for example documents that must be in original form.⁶¹ In any event, secure electronic signatures have not been widely adopted in the federal government, and certainly not for dealings with the public for which reference to PIPEDA would be necessary.

(d) Quebec legislation

Quebec did not implement the UECA, but instead adopted the *Act to provide a legal framework for information technology*.⁶² This Act shares with the UECA its media neutrality – it expressly approves of interchangeability of media – and its technology neutrality. It does not share the UECA's minimalism. Instead, it goes into considerable detail about the criteria needed for reliable use of e-communications. It defines a document (the Uniform Law Conference thought that went without saying) and spells out the need for document integrity during the life cycle of the document. It imposes a number of duties on the users of such “technological documents”.⁶³

Generally speaking, the Quebec statute will rarely produce a different legal obligation than the UECA, but the approach is distinct. One could even consider the Quebec Act as a kind of user's guide to the

than for Part 2 on electronic documents. Part 3 is discussed below with respect to electronic evidence at TAN 250.

56 Part 2 came into force on May 1, 2000. The designated Act is the *Federal Real Property and Federal Immovables Act*, S.C. 1991 c.50, and the regulation is the one made under that Act. See PIPEDA Part 2 Schedules B and C.

57 See for example PIPEDA s. 44 on statements made under oath, s. 45 on statements certifying the truth of information in the statement and s. 46 on witnessed statements.

58 See PIPEDA Part 2 section 48.

59 Secure Electronic Signature Regulations, SOR 2005/30.

60 A digital signature is an electronic signature created using asymmetric key cryptography. A PKI is a system of technical standards, rules and contracts that permit the wide use of digital signatures, generally using one or more trusted intermediaries between the signer and the person relying on the signature. For more information, see Treasury Board of Canada Secretariat, “PKI for Beginners”, online:

http://www.collectionscanada.gc.ca/webarchives/20071206022809/http://www.tbs-sct.gc.ca/pki-icp/beginners/beginners_e.asp, and “Government of Canada PKI”,

online:http://www.collectionscanada.gc.ca/webarchives/20071206022507/http://www.tbs-sct.gc.ca/pki-icp/gocpki/gocpki_e.asp. The current federal policies are online: <http://www.tbs-sct.gc.ca/sim-gsi/pki-tcp/pki-tcp-eng.asp>.

61 PIPEDA s. 42.

62 R.S.Q. c. C-1.1 (cited here as Quebec LFITA).

63 Quebec LFITA ss. 3 and 1: a document based on “information technology, whether electronic, magnetic, optical, wireless or other, or based on a combination of technologies.” A technological document is the same as what the UECA calls an electronic document. There is no difference in the scope of the two expressions.

UECA, in that it provides prudent counsel on matters to keep in mind in the electronic world. The Act is also more ambitious than the UECA, in that it goes beyond removing barriers to positive prescriptions about, among other topics, privacy, document preservation, the use of encryption, and the development of legal and technological standards. In these areas it may prove to be out in front of the rest of the country, in the direction we may all eventually move.⁶⁴

IV. ELECTRONIC COMMERCE

Thus in Canada much of the work has been done to remove the barriers to the legally effective use of electronic communications due to existing form requirements presuming paper. We now turn to a number of legal issues presented by e-communications generally, more because of their technical nature than because of existing legal rules to which they must conform.

1. Authentication and Signatures

Authentication addresses two questions: where did this record (or communications) come from, and is the record what it purports to be? Both are questions of evidence, though not necessarily of the formal law of evidence. Authentication of a person (a source) is often tied up in a question of signature, since a signature is evidence of a link between a document and a legal person.⁶⁵ (The form of the signature does not tell you what the link is, or what its own purpose is; for that, one needs the context of the document itself, or other evidence.) Signature technology can be as simple as a typed name at the bottom of an email⁶⁶ or as complex as a certified encryption key in the framework of a public key infrastructure.⁶⁷

Data authentication (as distinct from source authentication) works to ensure that the record has not been subject to intentional or unintentional modification. A number of techniques are available, including password protection, use of hard-to-modify software (Portable Document Format – PDF – is often cited for this purpose, though its security level varies), and cryptography, sometimes tied to a secure signature.⁶⁸

64 In this respect it would resemble the law of privacy for the private sector, in which Quebec legislated several years ahead of the rest of Canada.

65 There are many means of authenticating a document – electronic or not - that do not involve a signature, but the significance of an electronic signature attracts a good deal of discussion.

66 An Alberta court held that a series of emails with the names of the senders at the bottom satisfied the Statute of Frauds with respect to an agreement to transfer real estate, though in that case there was no dispute about the origin of the emails. *Leopky v Meston* 2008 ABQB 45. A Singapore court held that the headers on a series of emails satisfied the signature requirement of that country's version of the Statute of Frauds. *S.M.Integrated Transware v Schenker Singapore*, [2005] SGHC 58, [2005] 2 SLR 651. However, an English case found that an email address automatically inserted into an email by the Internet Service Provider (essentially the header) did not constitute a signature that could support a personal guarantee for the purposes of the Statute of Frauds. *J Pereira Fernandes SA v Mehta* [2006] EWHC 813, [2006] 1 WLR 1543 (Ch).

67 For more on public key infrastructure (PKI), the most frequently mentioned high-security authentication method, see the Government of Canada's site under the aegis of the Chief Information Officer: <http://www.tbs-sct.gc.ca/sim-gsi/pki-tcp/pki-tcp-eng.asp>, and the archive of the former PKI site referred to on that page.

68 More accurately, integrity may be demonstrated by calculating an abbreviated version of the digital text, called a 'hash value', by software that ensures that every text will produce a different hash value. To verify the integrity of the document, calculate the hash value of the document and compare it to the hash value of the original. Encryption is used to transmit the original hash value, to protect it against change.

In its essence, authentication involves a judgment on the credibility or reliability of a document. Making this judgment raises technical, legal and policy issues.⁶⁹ Authentication is a different question from that of legal effect: one judges the legal effect of a document after one knows how much one trusts it to have any effect, or whether authentication rules allow it to have any effect.⁷⁰

As a result, authentication questions come up in principle every time one uses an electronic document. In practice, of course, people rely on most electronic communications without worrying about their reliability. They do so because the risk is low, or the stakes are low, or their experience with the type of communications in question is satisfactory. In addition, people protect their systems as much as or more than they worry about particular records. Businesses generally have firewalls and anti-virus programs at work, and often add content-based filters. To these technical protections they add staff policies about risky uses of electronic communications. These days most Internet Service Providers offer considerable technical safeguards to their consumer customers too. As noted earlier, the more secure the system, the less one may have to worry about individual records in it.⁷¹

2. Electronic Contracts

The basic question that commerce faces with electronic communications is whether one can make a contract by electronic means. Businesses did not wait for law reform to go massively online, but some lawyers were cautious about giving opinions that such contracts were enforceable.⁷² If an oral contract is binding, with all its risks of inaccuracy, why should an electronic contract be less valid? In any event, the legislation referred to above dealt with this too. Section 20 of the UECA⁷³ says that an offer, acceptance or any other matter material to the formation or operation of a contract may be expressed by an electronic document or by an action in electronic form, such as touching or clicking on an icon or computer screen.⁷⁴

Indeed the UECA has an even broader permission. Section 5 provides that “Information shall not be denied legal effect or enforceability solely by reason that it is in electronic form.” Arguably the contract validation and much else in the Uniform Act flows from that one rule. Quebec has an equivalent rule.⁷⁵

The UECA also deals with three other possibly problematic features of e-commerce. First, it expressly allows transactions where one or both parties participate through automated systems, though in such

69 These are separated out in an Industry Canada publication, “Principles for Electronic Authentication: A Canadian Framework”, 2004, online: http://www.ic.gc.ca/eic/site/ecic-ceac-nsf/eng/h_gv00240.html.

70 For a fuller discussion of authentication, see John D. Gregory, “Authentication Rules and Electronic Records”, above, note 4. An international perspective is found in the work of the UNICTRAL Secretariat, *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*, (2007), online: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.

71 For the impact of these considerations on the practice of law, see the section below on that topic, TAN 279.

72 For example, Ontario's *Sale of Goods Act*, R.S.O. 1990 c. S.1, used to say in s. 5 that any executory contract for more than \$50 had to be in writing. Did e-contracts qualify? To avoid having to answer that question, the section was repealed in 1994. S.O. 1994 c.27, s. 54.

73 And all of its provincial implementing statutes except for New Brunswick's. New Brunswick thought it went without saying. New Brunswick Department of Justice Consultation Paper, December 15, 2000. The other UECA provisions mentioned here are generally common to all implementing jurisdictions.

74 Most of the UECA provisions discussed here were inspired by, or drawn directly from, the UN Model Law on Electronic Commerce, above note 24.

75 Quebec LFITA s. 5.

cases there is no simultaneous meeting of human minds usually thought essential to a contract.⁷⁶ Second, it provides a way out to the individual who makes mistake in dealing with an automated system, like a website, if that system does not allow an opportunity to avoid or correct the mistake.⁷⁷ The party making the mistake is not allowed to benefit from the transaction or to get out of it if a benefit has been provided and is not returnable.⁷⁸ Quebec has an equivalent provision, though with more express obligations as to the mechanisms to be provided by the merchant site.⁷⁹

The third characteristic of electronic communications of note here is the uncertainty about where and when e-messages are sent and received. Uncertainty arises because of the use of communications intermediaries like Internet Service Providers and others, because electronic addresses are less stable than physical ones, and because insecure communications can lead to messages being rendered unintelligible by malware, or filtered out by anti-malware technology.

The UECA therefore provides that a message is sent from and received at the place of business of the sender or addressee, rather than for example where the sender or recipient actually is at the relevant time (such as at a remote location, or using a mobile device).⁸⁰ The message is sent when it leaves the control of the sender, regardless of intermediaries, and it is presumed to be received when it enters the information system of the addressee – if the addressee has designated the address at that information system.⁸¹ One has no duty to check all possible communications systems. If the address has not been designated, then the message arrives when the addressee has notice of it. The presumption of receipt can be rebutted by showing the operation of a filter or the non-operation of the system at the relevant time. In short, the routines of paper communications are adjusted somewhat when they become electronic.⁸²

Generally speaking, the laws facilitating e-commerce like the UECA and the UN documents give a wide play to party autonomy.⁸³ Businesses are allowed to make their own deals and are expected to be

76 UECA section 21.

77 UECA section 22. The provision about error correction was borrowed from the American Uniform Electronic Transactions Act, National Conference of Commissioners on Uniform State Laws, 1999, s.10. See the commentary to that section online: http://www.law.upenn.edu/bll/archives/ulc/ecom/ueta_final.pdf p.38. A similar provision was included in the ECC, article 14, restricted to an “input error”. See J.D. Gregory and J. Remsu, “Error in Electronic Communication”, in Boss and Kilian, above note 25 p.198.

78 An online securities transaction could probably not be unwound once entered, so it might not benefit from this provision. It is still a good practice for web design to offer an opportunity to correct errors: “you have ordered X widgets, are you sure?”. Neither the UECA nor the ECC specify how this opportunity is to be presented.

79 Quebec LFITA s. 35.

80 UECA section 23(3), ECC article 10(3). Consider whether this creates a different result from a contract made by phone or letter by a party who is away from his or her usual place of business. Despite statutory rules, it is still helpful to specify the place the contract is made, or the applicable law of and forum for dispute resolution.

81 UECA section 23(1)(2), ECC article 10(1)(2). For a discussion of how one might designate an address, see W. Kilian, “Time and Place of Dispatch and Receipt” in Boss and Kilian, above note 25, p. 174. See also Quebec LFITA s. 31 para 2.

82 The UECA does not deal with the time at which a message has legal effect, as distinct from the time when it is presumed to be received. The legal effect was considered to be a rule of substantive law inappropriate for this statute about form. It seems that e-communications are considered to be delivered instantaneously and that the mailbox rule of common law acceptances does not apply to them. Thus the contract is made where and when the electronic acceptance is received. J.D. Gregory, “Receiving Electronic Messages”, (2000), 15 Can. Banking & Finance L.R. 473, online:<http://www.euclid.ca/bflr2000.pdf>.

83 In the UECA, several sections in the part on Communication of Electronic Documents apply unless the parties agree otherwise. See also MLEC article 4 and ECC article 3.

able to protect themselves.

The law of e-contracts goes beyond the questions of consent resolved by statute, however. Clicking on an “I agree” token is easily seen as showing consent, assuming that it can be proved later exactly what one consented to in doing so. It is a separate question whether one can enforce the terms of a web site that simply says “use of the site implies acceptance of these conditions”. The very few cases that have upheld such terms have typically done so against people who were taking information in ways that would clearly have been contrary to the interests, and thus the implied intent, of the owner.⁸⁴ In short, the clearer the consent to the terms to be enforced, the better for their enforcement.

3. Consumer Protection

By contrast, one of the main areas of concern in electronic commerce is the protection of consumers. Consumers generally have less knowledge of the risks of information technology than online merchants, so their vulnerability is thought to be greater than in traditional business – an area where special statutes have been widely adopted in any event. Federal, provincial and territorial ministers responsible for consumer matters have adopted principles⁸⁵ and a code of conduct⁸⁶ for good practice in online consumer transactions, directed both at merchants and at consumers themselves.

In addition, the same group developed a standard set of rules for online sales: the Internet Sales Harmonization Template.⁸⁷ This document has been given the force of law in most provinces.⁸⁸ It provides for thorough disclosure of key elements of a transaction before a contract is made, and provides for remedies for consumers when disclosure is not made or if performance is not forthcoming as agreed. Remedies include rescission of the contract and a right to charge back the price of the contract through the issuers of any credit card used in the transaction.

The Competition Bureau of Canada has noted that the laws of misrepresentation apply online. Its report on that issue outline some of the methods by which misrepresentation may be done, and says that it will enforce the rules in electronic as in bricks-and-mortar commerce.⁸⁹

The Office de la langue française in Quebec takes the view that its rules about offering goods and services to the Quebec market in French apply online as well to any vendor with a place of business in Quebec, even if the server is outside the province.⁹⁰ It has enforced this view successfully in the courts

84 C. Kunz et al., “Browse-wrap Agreements: Validity of Implied Assent in Electronic Form Agreements”, (2003), 59 *Bus. Lawyer* 279. Canadian law is likely to produce similar results. See *The Canadian Real Estate Association v Sutton* (2003) IIIJ Can. 22519 (QCSC)

85 *Principles of Consumer Protection for Electronic Commerce: a Canadian Framework* (1999), online: <http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00113.html>.

86 *Canadian Code of Practice for Consumer Protection in Electronic Commerce* (2004), online: [http://cmcweb.ca/eic/site/cmc-cmc.nsf/vwajp/EcommPrinciples2003_e.pdf/\\$FILE/EcommPrinciples2003_e.pdf](http://cmcweb.ca/eic/site/cmc-cmc.nsf/vwajp/EcommPrinciples2003_e.pdf/$FILE/EcommPrinciples2003_e.pdf).

87 *Internet Sales Contract Harmonization Template* (2000), online: <http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca01642.html>.

88 See the Uniform Law Conference's chart, right-hand column, online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4b>. Quebec has been added since the chart was made. See S.Q. 2006 c. 56.

89 Competition Bureau of Canada, *Application of the Competition Act to Representations on the Internet* (2003), online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/01213.html>.

90 Office de la langue française, “Frequently asked questions about the Charter of the French Language and web sites”

on more than one occasion.⁹¹

These issues are arising all over the world. A compendium of advice for consumers online prepared by the American Bar Association⁹² can usefully be read by Canadians as well. A companion site offers suggestions for online merchants⁹³ that are also largely applicable in Canada. Guidance in the European Union on unfair contract terms⁹⁴ could help both sides in an online transaction here.

Consumer notice questions have come up in other areas, such as whether consumers can be compelled to resolve disputes by arbitration, or to renounce rights to start a class action. The Supreme Court of Canada has been favourable to arbitration clauses,⁹⁵ assuming proper notice, but at least two provinces have legislated against imposing such provisions on consumers unfairly.⁹⁶

V. ELECTRONIC GOVERNMENT

Governments use electronic communications along with everyone else. They also have to govern a world full of such communications. This presents a number of legal challenges.⁹⁷

1. Government as user of e-communications

The first and easiest question is whether governments have the right to use electronic communications for their purposes. To remove all doubt, the general enabling legislation discussed above expressly permits governments to do so.⁹⁸ Government is subject to requirements about its information that do not apply to the private sector, however. For example, privacy rules tend to be different, and more

(1997), online: http://www.oqlf.gouv.qc.ca/english/infoguides/faqs/faqs_anglais.html#frequently.

91 *Quebec (procureur général) c. Hyperinfo* 2001 CanLII 16493 (QC C.Q.); *Québec (procureur général) c. Aroyan*, 2006 QCCQ 5922.

92 Online (appropriately enough): <http://www.safeshopping.org>.

93 Online: <http://www.safeselling.org>.

94 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, online: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31993L0013&model=guichett

95 *Dell Computers*, above note 15. For a U.S. decision in the other direction, see *Specht v Netscape*, 306 F.3d 17 (2nd circ., 2002). The American cases generally turn on the fact of notice, i.e. traditional contract idea of informed consent. A recent Texas decision refused to enforce an arbitration clause because the merchant had reserved the right in the contract to amend it unilaterally, thus making its own consent to the terms “illusory”, although the customer had clicked through an agreement to the terms and the terms had not in fact been amended since then. *Harris v Blockbuster*, (E. D. Tex. 2009), online: <http://iptablog.org/images/harris-v-blockbuster.pdf>.

96 Ontario, above note 17 s. 7; Quebec, *An Act to amend the Consumer Protection Act and the Act respecting the collection of certain debts*, S.Q. 2006 c.56, now s. 11.1 of the Act.

97 See P. Trudel, “The Development of Canadian Law with respect to E-government”, in J.E.J.Prins, ed., *Designing E-government*, 2nd ed., Kluwer 2006; John D. Gregory, “Solving Legal Issues in Electronic Government: Authority and Authentication”, (2002), 1 Cdn Journal of Law and Technology No. 2 p.1, online: http://cjlt.dal.ca/vol1_no2/pdfarticles/gregory.pdf, and “Solving Legal Issues in Electronic Government: Jurisdiction, Regulation, Governance”, (2002), 1 Cdn Journal of Law and Technology No. 3 p.1., online: http://cjlt.dal.ca/vol1_no3/pdfarticles/gregory.pdf. Electronic government can also include questions of governance, i.e. e-democracy, beyond the scope of this article D. Lenihan, *Progressive Governance for Canadians: What You Need to Know*, (Public Policy Forum, 2007), online: <http://www.ppforum.ca/sites/default/files/BOOK-Progressive%20Governance%20for%20Canadians.pdf>; and, among many other sites, <http://www.e-democracy.org>.

98 UECA section 17, PIPEDA section 33. The Quebec statute applies to all uses of information technology without speaking of particular classes of user.

extensive.⁹⁹ Archiving rules are unique to government, and the evolution of hardware and software makes storing electronic information over long periods difficult.¹⁰⁰

One of the main concerns of government in the electronic age is authentication. How does the government know where information that it receives is coming from, and whether it is what the sender intended to transmit? And how do users of official texts in electronic form know that the information actually comes from the government and can be relied on?

(a) Incoming documents

Governments have several techniques for dealing with authentication of incoming information. The first is not to try! Registering the names of businesses not using their corporate name, or of partnerships, used to be done in Ontario by submitting a signed form with the relevant information (and the relevant fee). No one ever checked the signature, and the consequences of a false registration had little public impact. As a result, there was little incentive to file false information. When the process became electronic, the signature requirement was simply dropped.¹⁰¹

The second technique is to close the system. In a closed system, everyone using e-communications has agreed to participate according to fixed rules, uses agreed software, and may also have a bank account from which applicable fees may be withdrawn automatically. All participants are identified when they join. This method works in Ontario for filing financing statements under the *Personal Property Security Act*¹⁰² and for land registration under the *Land Registration Reform Act, 1994*.¹⁰³ The rule is described in the *Electronic Registration Act (Ministry of Consumer and Business Services Statutes), 1991*.¹⁰⁴ Section 4(4) reads as follows:

Information that is filed in an electronic format may be filed only by a person who is or who is a member of a class of persons that is authorized to do so by a person who has the power to authorize such filings under a designated Act or, if no person is authorized under the designated Act, by the Minister.

A third method of ensuring authentication is to make the sender of the electronic information keep a signature on paper to certify its accuracy. In short, the government “outsources” the authentication function to the originator of the document. The paper signature must be produced if authenticity is questioned. This technique is used for electronic filing of securities documents under the SEDAR system run by the Canadian Securities Administrators.¹⁰⁵

99 All Canadian governments are subject to legislation on protecting personal information; not all jurisdictions have private sector privacy legislation, and the federal law on that topic (PIPEDA Part 1) is not comprehensive.

100 See the International Research [Project] on Permanent Authentic Records in Electronic Systems (InterPARES), online: <http://www.interpares.org/>.

101 The *Business Registration Reform Act, 1994*, S.O. 1994 c.32, s. 10 authorized the Minister by regulation to dispense with signatures otherwise required or to provide for methods to be used to sign electronically. This power was exercised with respect to the *Business Names Act*, R.S.O. 1990 c. B.17, by Ontario Regulation 442/95. Several other provinces have similar legislation.

102 R.S.O. 1990 c. P.10. Electronic filing – without signatures – was authorized by O.Reg. 75/92.

103 R.S.O. 1990 c. L.4. See ss 20(2) and 23(2) for the Director's control of who participates in the system

104 S.O. 1991 c. 44.

105 See http://www.sedar.com/homepage_en.htm for details.

A further method of dealing with legally secure authentication is to allow a case-by-case discretion to rely on satisfactory technology. One may think of the *Income Tax Act*,¹⁰⁶ which permits electronic filing of tax returns by “using electronic media in a manner specified in writing by the Minister of National Revenue.”¹⁰⁷ The specification spells out that using the three means of identification provided in the program constitutes the taxfiler’s signature.¹⁰⁸ In Ontario, the *Compulsory Automobile Insurance Act*,¹⁰⁹ permits the use of any signature approved by the Minister.¹¹⁰

Finally, the use of electronic authentication is sometimes authorized expressly by Act or regulation to be used in connection with the purposes of the Act. The *Provincial Offences Act*¹¹¹ says this:

76.1(1) A document may be completed and signed by electronic means in an electronic format and may be filed by direct electronic transmission if the completion, signature and filing are in accordance with the regulations.

Those regulations are more concerned with function than with form.¹¹²

The *Business Corporations Act*¹¹³ requires reliability, but does not define it:

110(4.2) A shareholder or an attorney may sign, by electronic signature, a proxy, a revocation of proxy or a power of attorney authorizing the creation of either of them if the means of electronic signature permits a reliable determination that the document was created or communicated by or on behalf of the shareholder or attorney, as the case may be.

(b) Outgoing documents

That is a quick overview of how government authenticates incoming information. What of electronic records coming from government that their users need to know are genuine? There are two basic methods: a unique identifier and a secure electronic signature.

The unique identifier is a reference number embedded in an electronic record, unique to that record as its name suggests, that refers back to a secure public database. Someone who wants to verify the information in the record can go independently to the database and see if the official information is the same as that tendered. The ease of checking deters fraudulent alteration of the record. Thorough security is needed for the database itself for this process to be reliable.

This system is used by the Companies Branch of the Ministry of Government Services, for certificates

106 R.S.C.1985 c.1 (5th supp.).

107 *Ibid.* s. 150.1.

108 Netfile security guideline, online: <http://www.netfile.gc.ca/scrty-eng.html>. The three identifying items are the filer’s Social Insurance Number, birth date and Access Code provided by the Canadian Revenue Agency. The software used to file is tested every year as well.

109 R.S.O. 1990 c. C.25.

110 O.Reg. 278/95. The Minister has approved an electronic signature created by pressing on an “I agree” icon on the screen of a Service Ontario kiosk, to certify that one has valid auto insurance when one is renewing a licence plate tag at the kiosk. Text on the screen explains the significance of pressing the icon.

111 R.S.O. 1990 c. P.33

112 *Provincial Offences Act*, Electronic Documents Regulation, O.Reg. 497/94.

113 R.S.O. 1990 c. B.16.

of status attesting to the existence of Ontario corporations and their directors and officers. The Ministry of the Attorney General uses a similar system for electronic writs of seizure and sale. The unique identifier links to the court's database so one can tell if a judgment was entered against the apparent judgment debtor and for what sum. Having the writ in electronic form allows for its filing in the electronic land register without ever taking paper form.

The writ of seizure and sale is a court document, and the *Courts of Justice Act*¹¹⁴ requires such documents to have a seal.¹¹⁵ The Attorney General has approved the unique identifiers as the seal for electronic writs. Indeed they provide better authentication than the physical seal embossed on paper, which identified only the name of the court and which might be duplicated without much effort.

The same principle is found internationally. The Hague Legalisation Convention¹¹⁶ provides for an authentication certificate called an "apostille" to be affixed to public documents to be used in other countries. The issuers of apostilles are required to keep a register of all the apostilles they issue, so that recipients in foreign countries can check the authenticity of apostilles they receive. At present, with apostilles on paper, almost no one ever checks.¹¹⁷ As public documents become electronic and are authenticated by electronic apostilles, the availability of an electronic register to verify these apostilles, readily accessible from anywhere in the world, becomes a keystone of a reliable system.¹¹⁸

The federal government's statute, PIPEDA,¹¹⁹ permits seals to be created electronically by a secure electronic signature. As noted above, such a signature relies on cryptography under the Government of Canada Public Key Infrastructure. Cryptography is the second method that governments use to permit the authentication of their e-records. Traditional encryption that depends on a shared secret, the key to encrypting and then decrypting the information, works well between two people. If one can read the document, one has a good degree of certainty that it was created by the other. However, shared or symmetrical cryptography does not work well for large numbers of people who create and who must read e-records. The management of the keys, distributing them and keeping them secret, is very difficult. Proving which holder of the shared secret actually signed a document can be a challenge too.

Asymmetric or dual-key cryptography has been seen as the solution. A record is encrypted with one key and read with another. The two keys are mathematically linked so that only one of the pair can decipher what the other has encrypted, yet if one knows one key it is not feasible to figure out the other.¹²⁰ This method can therefore be used as a signature. If one knows who holds the signing key, one can be sure that the document one can read with the corresponding decryption key must come from that person. The decryption key does not have to be secret; it is generally known as the public key, corresponding to the private key that is the secret of its holder. The keys work in one direction for

114 R.S.O. 1990 c. C.43.

115 Ibid. s. 147.

116 Convention of 5 October 1961 Abolishing the Requirement of Legalization for Foreign Public Documents, online: http://hcch.e-vision.nl/index_en.php?act=conventions.text&cid=41.

117 Synopsis of replies to Questionnaire, Preliminary Document No. 6, November 2003, online: http://hcch.e-vision.nl/upload/wop/lse_pd06.pdf, page 15.

118 The Hague Conference on Private International Law's information site on the "e-APP": <http://www.e-app.info>, notably "What is the e-APP?", online: http://www.e-app.info/Education/English/a001_e_apostilles_section_page_1_of_5.html.

119 Above note 55.

120 See the sources cited above in note 60.

authentication and in the other for confidentiality, the traditional use of encryption. A document signed by the private key must have been signed by the known holder of that key (absent fraud or negligence); a document signed by the public key can be read only by the holder of the private key.

The problems of key management in public key cryptography are to ensure that private keys are kept private and to communicate to the appropriate number of people just who does hold the private key associated with a public key. Ensuring secure handling is a matter of prudence, contract and sometimes law.¹²¹ Communicating the identity of the key holder is sometimes assigned to a trusted third party, or certification authority, that certifies the association. In such a public key infrastructure, why should one trust the “trusted” third party? Sometimes there is a chain of trust leading to someone known to be reliable; sometimes the certification authority at the end of the chain is the government itself.

At present, PKI is not yet widespread for governments communicating with the public. Governments often need to communicate with large numbers of people, and not all of the target audience may have the capacity to verify digital signatures.¹²² Managing a PKI is not easy either. To date most governmental uses of this authentication method have been within the public sector, where both authentication and the need for confidentiality support the expense. For example, two uses known in Ontario are from one police force to another and among the Ministry of Community and Social Services and Children’s Aid Societies.¹²³

One can conclude that authentication in dealing with government is not yet routine for all purposes. The methods and the legal support for them are varied and still in evolution. As a result, the same is true of governmental uses of e-communications in general.

2. Governing electronically

What do governments do? In a small nutshell, governments try to affect who does what and how, to maintain peace, order and good government, to promote public welfare and perhaps to facilitate the pursuit of private happiness. The electronic world presents a number of challenges for these mandates, since it is sometimes hard to know in respect to cyberspace just where anyone is and who is doing what to whom, and how. Thus governments may not know that problems exist or that rules are being broken, and even if they know, they may have limited access to the source of the problem. This is true even when the participants in the online world are in the territory of the government, and all the more so when they are or could be anywhere else in the world.

Governments have attempted to meet these challenges in diverse ways and with differing degrees of success. We will look at these responses through questions of dispute resolution and of regulation.

121 Legislation validating public key cryptography may invalidate a signature, or at least not require reliance on it, if the holder of the private key is shown not to have handled it with due care. See for example the UN Model Law on Electronic Signatures, U.N. Resolution Doc. 56/80, December 12, 2001, U.N. Document A/56/588, online: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>, article 6(3)(a).

122 Recent versions of Adobe’s Portable Document Format writers have the power to create digital signatures and certificates, though, so the ability to verify may become more widespread.

123 For information coming into government, PKI is used in Ontario’s electronic land registration system. Lawyers are issued digital signature keys, and securely communicate to the land registry the instructions for dealings in the land. These signature keys are of no use for communicating to anyone else, even among lawyers within the system, since no one but the land registry has the verification key. That is why the system was described earlier as closed.

Dispute resolution occurs in public institutions like courts and administrative tribunals. Regulation can pass through those bodies but also involves alternative methods, a search for proxies and indirect pressures.¹²⁴

(a) Dispute resolution

Courts have of course dealt with questions of jurisdiction since the earliest times, well before the days of cheap and easy transportation, much less of electronic communications. But it is one thing to know how to deal with a party who is outside the territory of the court. It is another to figure out how to deal with a party who is outside and inside at the same time, or in many or even all jurisdictions at the same time, especially one that does not have a physical presence in the court's territory.¹²⁵

The first response by courts dealing with suits against parties on the Internet was to resist a broad reach. The mere accessibility of information on the Internet was not enough to give a real and substantial connection with the court.¹²⁶ The better view was that a court would assert jurisdiction over a party running a web site, for example, if the site provided for interactivity with people in the court's territory. Interactivity suggested an intention of the online party to avail itself of commercial opportunities in the territory, and it could not come as a surprise that there might be legal consequences of doing so.¹²⁷

In time, perhaps because technology evolved to make interactivity trivial, courts started looking more closely at the intention of the online party. It became important to consider if that party had "targeted" the court's territory, or a party in the territory.¹²⁸ Even more than in commercial disputes, this view took hold in defamation cases. One of the leading cases came out of the High Court of Australia, which allowed a resident of New South Wales to sue an American publication on the ground that the publisher knew that the defamatory statements were read where they would do damage, namely in Australia, and thus it was appropriate that the victim should claim a remedy there.¹²⁹ Similar findings have been made in English courts.¹³⁰

However, courts were still able to decide that the connection was too remote. The Ontario Court of

124 Further detail can be found in Coughlan, Currie, Kindred and Scassa, "Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization", (2007), 6 Cdn Journal of Law and Technology No. 1 p.29, and in J. D. Gregory, "Internet Jurisdiction: Where Are We Now?", presentation to the Toronto Computer Lawyers Group, November 2005, linked to online: <http://www.tclg.org/past-meetings/2005-nov.html>.

125 Some people have tried to avoid these issues by resolving disputes electronically. Online dispute resolution (ODR) has had a number of apparent launches, including a thorough review by the American Bar Association between 2000 and 2002. A PowerPoint report of this initiative is online: http://apps.americanbar.org/buslaw/newsletter/0008/adr/adr_task_force.pdf. For more information, see online: <http://www.odr.info>.

126 See for example *Compuserve v Patterson*, 89 F.3d 1257 (1996)(6th circuit).

127 This is known as the Zippo test, after a case in which it was clearly formulated. *Zippo Manufacturing Co. v Zippo Dot Com*, 952 F. Supp. 1119 (W.D.Pa., 1997) This approach was approved in Canada in *Braintech v. Kostjuk*, 1999 BCCA 0169, online: <http://www.courts.gov.bc.ca/jdb-txt/ca/99/01/c99-0169.txt>, leave to appeal denied by SCC.

128 This development was examined in M. Geist, "Is There a There There? Toward Greater Certainty for Internet Jurisdiction", (2001) online: <http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf>.

129 *Dow Jones v Gutnick*, [2002] HCA 56 (High Ct of Australia)

130 See for example *Lewis v King* [2004] EWCA Civ 1329.

Appeal in *Bangoura v Washington Post*¹³¹ found that Ontario was not sufficiently connected to the facts, where an American newspaper had published defamatory remarks about an African living in Africa at the time of publication. That the victim had since moved to Ontario and that the remarks were still available in an electronic archive were not sufficient basis for an Ontario lawsuit. The *Bangoura* decision may show a move away from the “targeting” principle to a more conventional application of the usual jurisdictional tests of real and substantial connection to activities in cyberspace.¹³² For example, the Federal Court of Appeal has reviewed the traditional case law of ‘real and substantial connection’ from *Morguard*¹³³ to *Muscutt*¹³⁴ in finding none in an Internet case.¹³⁵

Law reformers have stepped in to help. Thus the Hague Conference on Private International Law has recently adopted a convention on Choice of Court Agreements.¹³⁶ The Uniform Law Conference has adopted rules for determining jurisdiction in consumer contract disputes.¹³⁷ The Organization of American States is working on a similar project.¹³⁸ Among the most ambitious projects has been the pair of Rome Conventions of the European Union to set rules for choice of court and law for consumer contracts and for non-contractual disputes. The contract rules (Rome I) have been the more difficult; after many years of effort, the treaty was finally adopted in early 2009.¹³⁹

Administrative tribunals have also had to decide on their reach. Here are four Canadian examples:

- The Canadian Radio-Television and Telecommunications Commission (CRTC) decided some years ago not to try to regulate the Internet itself, though it said it had the legal right to do so.¹⁴⁰ It said that there was enough choice and easy of entry into Internet publishing – even before the spread of blogs and user-generated videos – that restrictions were not needed to protect the values it needed to protect. The Commission reiterated this approach in June 2009.¹⁴¹ It may still oversee more focused issues. For example, it has recently launched an inquiry on “net neutrality”, the requirement that primary carriers of Internet traffic should give fair and equal access to the

131 *Bangoura v Washington Post* 2005 CanLII 32906 (ON C.A.)

132 For more on defamation online, including a discussion of jurisdiction, see E. Judge, “Cybertorts in Canada: Trends and Themes in Cyber-Label and Other Online Torts”, [2005] *Annual Review of Civil Litigation* 149, and more recently D. Burnett and H. Maconachie, “Defamation Law: Shifting Ground”, [2008] *Annual Review of Civil Litigation* 263, 288.

133 *Morguard Investments v De Savoye*, 1990 CanLII 29 (S.C.C.), [1990] 3 S.C.R. 1077.

134 *Muscutt v Courcelles*, 2002 CanLII 44957 (ON C.A.), (2002), 213 D.L.R. (4th) 577 (Ont. C.A.)

135 *Desjean Estate v Intermix*, CanLII 2007 FCA 365, affirming *Desjean v Intermix*, CanLII 2007 FC 1395 (FCTD).

136 The Hague Convention on the Choice of Court Agreements (2005), online:

http://www.hcch.net/index_en.php?act=conventions.text&cid=98 This Convention was what was left of a largely unsuccessful attempt to agree internationally on court jurisdiction and enforcement of judgments.

137 Uniform Law Conference of Canada, “Jurisdiction and Consumer Protection in Electronic Commerce Project”, report 2004, online: http://66.51.165.111/en/poam2/Jurisdiction_CP_E-Commerce_Enf_Judg_Paper_En.pdf.

138 The documents proposed on jurisdiction for the as-yet-unscheduled seventh OAS conference on private international law, CIDIP-VII, are online: http://www.oas.org/dil/CIDIP-VII_topics_cidip_vii_consumerprotection_jurisdiction.htm. Canada has a proposal based largely on the Uniform Law work mentioned in the previous footnote.

139 The Rome Convention of 1980 on the Law applicable to contractual obligations became a regulation of the European Parliament and Council COM(2005) 650 final, 2005/0261 (COD) published on 15 December 2005, online: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0650en01.pdf.

140 CRTC New Media decision, May 1999, online: <http://crtc.gc.ca/eng/archive/1999%5CPB99-84.htm>.

141 Broadcast Regulatory Policy CRTC 2009-329, June 4, 2009, online: <http://www.crtc.gc.ca/eng/archive/2009/2009-329.htm>.

networks by competing service or content providers.¹⁴²

It may be noted that much of the physical infrastructure of the Internet and the market conduct of the participants such as telephone and cable companies are subject to regulation. The infrastructure and major players are physically in Canada. There is little regulation of content of messages, however, beyond a concern for availability of Canadian content¹⁴³ and for fair opportunity to make political messages heard.¹⁴⁴

- The Alberta Securities Commission made orders in 1999 against the World Stock Exchange, although the company was registered in the Cayman Islands and its servers were located in Antigua.¹⁴⁵ The principals of the WSE and of some of its customers were in Alberta. The Commission noted that a network of agreements among securities regulators ensured the proper respect for the jurisdiction of each. However, it was not appropriate for the WSE to be regulated by no one. There was no better jurisdiction to regulate than Alberta.
- The Copyright Board has had to decide whether communication of music online occurred in or outside Canada, to decide when copyright royalties were payable. The Board focused on where the computer servers were. However, higher courts up to the Supreme Court of Canada held otherwise: the location was not relevant.¹⁴⁶ The place of business is among the key factors in determining a real and substantial connection – a civil litigation concept that has crept over into administrative law.
- The Canadian Human Rights Tribunal decided in 2002 that hate literature appearing on a web site based in the United States was still capable of violating a Canadian statute by use of telecommunications because the controlling mind was in Canada.¹⁴⁷ The ability to enforce the decision was not the controlling factor; it was hoped that foreign authorities might help enforce though they were not obliged to do so. After the decision the *Telecommunications Act*¹⁴⁸ was amended to express the Tribunal's jurisdiction in such cases.¹⁴⁹

(b) Regulation

Governments do more than provide resolution of disputes. They actively regulate behaviour. But their commands run only in their physical territory, and then only if they know of the activity and can find the actor. Rules can be created requiring, for example, that anyone carrying on an activity must be

142 CRTC Notice of consultation and hearing, November 20, 2009, "Review of the Internet traffic management practices of Internet service providers", online: <http://www.crtc.gc.ca/eng/archive/2008/pt2008-19.htm>.

143 CRTC mandate for Canadian content, online: <http://www.crtc.gc.ca/eng/cancon/mandate.htm>.

144 CRTC "Election Campaigns and Political Advertising", November 2008, online: http://www.crtc.gc.ca/eng/INFO_SHT/b309.htm.

145 *In the matter of the World Stock Exchange et al.*, (2000) 9 ASCS 658, online: http://www.albertasecurities.com/Enforcement/Enforcement%20Orders/1876/World_Stock_Exchange_-_Reasons_-_2000-02-15_-_1310963.pdf.

146 *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, 2004 SCC 45.

147 *Citron v Zundel*, January 18, 2002, online: http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=252&lg=e&isruling=0.

148 S.C. 1993 c. 38

149 S.C. 2004 c. 25 s. 174 expanded the definition of "telecommunications".

registered or licensed, and have a physical location in the territory for enforcement purposes. However, one is still left to deal with those outside the jurisdiction who insist on dealing with people within it without complying with those rules.

Governments have developed a number of techniques for dealing with this challenge. One of the main ones is to apply the rules to intermediaries that are physically present in the territory and thus subject to the usual legal sanctions for non-compliance. These intermediaries are sometimes involved in the technological structure of the Net, notably Internet Service Providers. Efforts have been made to require ISPs to detect and sometimes to sanction customers who infringe copyright in movies or music.¹⁵⁰ People have sued ISPs for defamation transmitted through them, though generally speaking the ISPs have been held not liable unless they hosted the defamatory material rather than just transmitting it.¹⁵¹ Recently it was held that a web site that linked to defamatory material was not liable in defamation if it did no more than link, i.e. it did not assert that the defamation was accurate.¹⁵²

The United States absolved communications intermediaries of most liability in 1996 legislation, in order to encourage the services provided.¹⁵³ In Canada, only Quebec has legislated directly on ISP liability, reproducing the result generally obtained in the common law.¹⁵⁴ The Tariff 22 decision of the Copyright Board, upheld by higher courts, found that ISPs were not responsible for retransmitting infringing copyright material.¹⁵⁵

Financial intermediaries are a frequent target of governments that seek to regulate online activities, since many online transactions rely on credit cards or other payment facilities. Issuers of credit cards have contracts with cardholders and with all merchants in their system, so issuers in the jurisdiction may be used to pressure those outside. Examples include the Internet Sales Harmonization Template mentioned above,¹⁵⁶ which allows consumers dissatisfied with violations of the rules to charge back the payments through their credit cards. The United States has led a serious campaign against Internet

150 United Kingdom: M. Horten, "UK Music companies demand ISP liability in copyright law", IPTegrity.com, January 28, 2009, online: <http://www.iptegrity.com/index.php/digital-britain/235-uk-music-companies-demand-isp-liability-in-copyright-law>; France: N. Anderson, "France reintroduces three-strikes law, clash with EU likely", Ars Technica, April 29, 2009, online: <http://arstechnica.com/tech-policy/news/2009/04/france-reintroduces-three-strikes-law-as-protests-mount.ars>; New Zealand: N. Anderson, "'3 strikes' strikes out in NZ as government yanks law", Ars Technica March 23, 2009, online: <http://arstechnica.com/tech-policy/news/2009/03/3-strikes-strikes-out-in-nz-as-government-yanks-law.ars>.

151 A. Bernstein and R. Ramchandani, "Don't Shoot the Messenger! A Discussion of ISP Liability", (2002) 1 Cdn Journal of Law and Technology No 2, online: http://cjltd.dal.ca/vol1_no2/pdfarticles/bernstein.pdf.

152 *Crookes v Wikimedia Foundation*, 2008 BCSC 1424. A similar finding had been made earlier about a printed link to a web site: *Carter v B.C. Federation of Foster Parents Asscn*, 2005 BCCA 396.

153 See section 230 of the *Communications Decency Act*, Title V of the *Telecommunications Act 1996*, 47 U.S.C. sec. 230.. The provisions has had the desired effect in most cases – sometime denying a remedy where serious injury has been done. *Zeran v American Online Inc*, 129 F.3d 327 (4th Cir. 1997), online: <http://caselaw.findlaw.com/us-4th-circuit/1075207.html>. A few exceptional cases have found liability where the ISPs were considered to have participated actively in the improper activities. *Fair Housing Council of San Fernando Valley v. Roommates.com, L.L.C.*, 489 F.3d 921 (9th Cir. 2007).

154 Quebec LFITA s. 36 says that intermediaries are not liable unless they knowingly participate in the doubtful activity. Compare the European Union's Directive 2000/31/EC on Electronic Commerce, recitals 43 – 48 and articles 12 – 15, largely to the same effect. Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>.

155 Above note 146.

156 Above note 87.

gambling by requiring financial institutions to detect and block many gambling payments.¹⁵⁷

Another intermediary targeted to enforce criminal law is the advertising business. Thus Ontario recently amended the *Consumer Protection Act, 2002*¹⁵⁸ to ban the advertising of gaming sites on the Internet that were operated contrary to the *Criminal Code of Canada*.¹⁵⁹ The ban applies to advertising that originates in Ontario or is primarily intended for Ontario residents.¹⁶⁰ It is not necessary to prove that the gaming sites themselves target Ontario. The advertising itself may be in print, broadcast or online.¹⁶¹

The American federal government worked to reduce access by minors to inappropriate web sites by requiring libraries to install filters, at the risk of losing their federal operating grants if they refused. This measure was upheld in court.¹⁶² Other US governments have required transportation companies to disclose the people to whom they have delivered goods bought online, where the goods were subject to state restrictions (such as alcohol or tobacco) or on which state tax would be payable if bought in person.¹⁶³

Recently the Canadian government required eBay Canada to disclose the names of “power sellers”, so the Canada Revenue Agency could determine if those people were declaring all their income for tax purposes. The Federal Court of Appeal upheld the request for these records, though they were stored outside the country, since they were retrievable by the Canadian operation.¹⁶⁴

It is worth mentioning briefly a few non-enforcement methods by which governments may seek to overcome the jurisdictional or enforcement limits of the Internet. One is harmonization of the law, which reduces the chances that someone in another jurisdiction may be permitted to do something forbidden here. We noted earlier the Internet Sales Harmonization Template as an example of provincial harmonization.¹⁶⁵ Most privacy statutes in developed countries derive from the OECD 1980 Guidelines for the Protection of Personal Data.¹⁶⁶ The Council of Europe Convention on Cybercrime,

157 *Unlawful Internet Gambling Enforcement Act*, U.S.Code ss. 5361 – 5367 prohibits financial institutions from facilitating transactions involving illegal Internet gaming facilities. The regulations say how it is to work. They were adopted in November 2008 and come into force on December 1, 2009. See Federal Register, Title 12 Banks and Banking, Part 233, Prohibition on Funding of Unlawful Internet Gambling.

158 S.O. 2002 c. 30 Sched. A..

159 *Ministry of Governments Service Consumer Protection and Service Modernization Act, 2006*, S.O. 2006 c. 34, s.8, creating a new section 13.1 of the *Consumer Protection Act, 2002*.

160 *Ibid.*, new section 13.1(3).

161 *Ibid.*, new section 13.1(4)(a).

162 *American Library Association v the United States*, 539 U.S. 194 (2003).

163 See for example the US General Accounting Office, *Internet Tobacco Sales: Giving AFT Investigative Authority may Improve Reporting and Enforcement*, (2002) Doc. GAO-02-743, online:<http://www.gao.gov/new.items/d02743.pdf>. The Jenkins Act discussed in this paper dealt with pre-Internet cross-border tobacco sales. State governments have tried numerous legal tactics to recover lost taxes. Recent New York City efforts are described in J. Stashenko, “New York City’s Use of Consumer Fraud, Public Nuisance Statutes to Recoup Cigarette Taxes Is Rejected”, Law.com, June 10, 2009, online (behind a LexisNexis paywall): <http://www.law.com/jsp/article.jsp?id=1202431350309>.

164 *eBay Canada Ltd v Canada (National Revenue)*, 2008 FCA 348 (CanLII). For more on the challenges of Internet transactions to the tax system, see J.D. Gregory, “Solving Legal Issues in Electronic Government: Jurisdiction, Regulation, Governance”, above, note 97, pp 2-13 and sources cited there.

165 See above, note 87.

166 Organization for Economic Cooperation and Development, *Guidelines governing the protection of privacy and transborder flows of personal data* (1980) online:

to which Canada is a party, ensures that member states take similar approaches with similar tools when dealing with criminal activity online.¹⁶⁷

Governments also encourage people to protect themselves from risks that governments cannot prevent directly. Consumer education sites have already been mentioned.¹⁶⁸ Securities regulators have made their education techniques diverse and attractive,¹⁶⁹ including an animated cartoon on becoming a gazillionaire,¹⁷⁰ though the game “Spot the Bull” seems to have disappeared.¹⁷¹

Finally, governments can create safe “places” online where people can “go” to avoid the security and privacy risks of the Internet at large. These “virtual communities” provide goods and services from merchants who have agreed to be regulated, because the merchants’ government-enforced good behaviour is a marketing advantage for them. The merchants must be in some way subject to traditional regulation by governments, either because they are in the territory controlled by the governments in question, or perhaps because they have submitted a bond or other security for their good behaviour.¹⁷² Such a program might be beneficial to the regulating government economically, as well as providing the satisfaction of regulating successfully. For example, the United Kingdom aimed to derive high-tech jobs and income from allowing Internet gaming operations in its country.¹⁷³

The safe community method was used first by private sector operations. America On-Line offered guarantees of fair dealing with all merchants that it allowed to operate on its system; the merchants would comply for the sake of access to the large numbers of users.¹⁷⁴ Amazon.com and eBay have had online dispute resolution systems for their users.¹⁷⁵ The Better Business Bureau set up an online system for its members and their customers.¹⁷⁶ For the Internet itself, a number of certification programs testify to its safety. One of the best known was created by the Canadian Institute of Chartered Accountants and its American counterpart: WebTrust.¹⁷⁷ It may be noted that voluntary codes of good

http://www.oecd.org/document/20/0,3746,en_2649_34255_15589524_1_1_1_1,00.html

167 Council of Europe Convention on Cybercrime, Budapest November 23, 2001, online:

<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

168 See above, TAN 92.

169 See the Ontario Securities Commission’s site <http://www.getsmarteraboutmoney.ca/Pages/default.aspx>

170 <http://www.lavamind.com/gaz.html>. The link to this site is on the OSC investor education site, above.

171 The press release announcing the game was online for some time after the the game itself, formerly at http://www.osc.gov.on.ca/en/games/spot_the_bull/index.htm, disappeared. Perhaps the disappearance of bull markets in 2008 made it inappropriate.

172 Such a plan was proposed by Professor Geist to the Ontario government in 2000. See M. Geist, “Consumer Protection and Licensing Regimes Review: The Implications of Electronic Commerce”, online at <http://aix1.uottawa.ca/~geist/mccrgeist.pdf>.

173 See the *Gambling Act, 2005 (U.K.)*, online: http://www.opsi.gov.uk/acts/acts2005/ukpga_20050019_en_1. Its operation in practice drew a blog comment from “Perfect Storm: UK Online Gambling Voice” in January 2009, online: <http://www.cashcade.co.uk/2009/01/12/online-gambling-regulation>. Professor Post hypothesized about this advantage in “Betting on Cyberspace”, *The American Lawyer* (June 1997), online: <http://www.temple.edu/lawschool/dpost/Gambling.html>.

174 AOL.com’s ‘total satisfaction’ program now appears to have been discontinued.

175 Amazon.com offers an “A to Z Guarantee”, described online:

http://www.amazon.com/gp/help/customer/display.html/ref=hp_navbox_inpriv_az?nodeId=537868. Ebay Canada offers an “Items not received service”, described online: <http://pages.ebay.ca/securitycentre/itemnotreceivedprocess/index.html>

176 Online: <http://www.bbb.org/us/partnerships/bbonline-trustmark-program> for the “trustmark” program. Nearly 52,000 websites meet this standard at time of writing.

177 See “Trust Services Principles and Criteria”, online <http://www.cica.ca/service-and-products/business->

online conduct are not new. Industry Canada published a guide to their development and use in 1998.¹⁷⁸

One final note is called for, on quasi-private enforcement of ‘regulatory’ standards. One describes as quasi-private the bringing of civil litigation to enforce statutory security or privacy rules, goals that are decreed by the government in legislating the standards. Common law standards of care may also be invoked. Thus nearly three-quarters of Canadian businesses surveyed said that their investments in privacy and security were prompted by legislation requiring results, and the fear of what would happen to them if they did not comply.¹⁷⁹ It has also been suggested by a noted expert on information security that only imposing civil liability on software developers will spur them to ensure that their products are secure before they release them to the public.¹⁸⁰

Thus governments need not and do not throw up their hands in despair because the activities they seek to regulate go online. These activities do not quite disappear in cyberspace, and there are ways of influencing their behaviour there.¹⁸¹

VI. LITIGATION ISSUES

The foregoing discussion of civil liability as a regulatory or enforcement technique turns our attention to the ways in which electronic communications and records have affected the practice of civil litigation itself. We look at four here: the use of electronic communications in litigation, electronic discovery, electronic evidence generally and the safe use of these technologies in the practice of law.

1. Electronic Communications

(a) Service

A lawsuit begins with the issue of some kind of originating process, like a writ, a statement of claim or an application to a court. In almost every case that document must be served on the other party or parties to the litigation, to ensure that all sides of the dispute have a chance to be heard by the decision-maker. Since the document will be created electronically these days, can one save on printing and

[opportunities-for-cas/trust-services/item10796.pdf](http://www.truste.com). The Electronic Frontier Foundation created “TrustE” for the same purpose. Online: <http://www.truste.com>.

178 Industry Canada, “Voluntary Codes – A Guide to their Development and Use” (1998), online: <http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00863.html>.

179 W. Hejazi and A. Lefort, “Rotman-TELUS Joint Study on Canadian IT Security Practices” (annual), online: <http://www.rotman.utoronto.ca/securitystudy>. For this statistic, see the 2008 study, page 28.

180 B. Schneier, “Computer Security and Liability” (Nov. 3, 2004), online: http://www.schneier.com/blog/archives/2004/11/computer_security.html. T. Espiner, “EC wants software makers held liable for code”, Cnet News, May 9, 2009, online: http://www.cnet.com/8301-1001_3-10237212-02.html?tag=newsEditorsPicksArea.0. An interesting speculation whether computer users, especially businesses, may be liable for not keeping their security measures up to date, if their systems become infected as a result and in turn pass on the infection to computers linked to theirs. See R. Owens, “Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections”, (2004), 3 Canadian Journal of Information Technology No. 1 p. 33, online: http://cjilt.dal.ca/vol3_no1/pdfarticles/owens.pdf.

181 This point was made in one of the first serious Canadian studies of law and the Internet. See Racicot, Trudel, Szibbo and Hayes, “The Cyberspace is not a ‘no-law land’”, published by Industry Canada in 1997, online: <http://archive.ifla.org/documents/infopol/canada/icrls.pdf>.

serve it electronically?

The answer so far in Canadian law, and in most if not all other legal systems, is No. Courts insist on certainty that the other party has notice of the litigation, and they satisfy that insistence by having sworn evidence that the party has been served. That evidence is given by way of personal knowledge of the person carrying out the service. Present technology does not guarantee that the addressee of electronic communication has received it. If both parties use the same software, their systems may be capable of generating and receiving a receipt, but the rules of civil procedure cannot be built on chance compatibility of computer systems.

We noted in our discussion of electronic commerce that the UN Model Law on Electronic Commerce and its Canadian implementing legislation in common law jurisdictions provide a presumption of receipt when an electronic message enters the information system designated by the addressee.¹⁸² This provision cannot support electronic service for two reasons. First, the addressee may not have designated any system for the purpose of receiving legal notices, especially ones adverse in interest. The Model Law and its progeny do not create a duty on anyone to become aware in a timely way of anything sent to them by any possible message system. Thus a message sent to an undesignated system is not received under the statutes until the addressee becomes aware that it is available. That is not an acceptable standard for service of originating process, especially when legal consequences may flow from a failure to respond within a fixed time.

The second reason that the Model Law statutes do not support electronic service is that even with a message sent to a designated system, there is only a presumption of receipt. Many things can go wrong, including a system failure at either end or in the middle – and Internet communications may have a very broad middle. Communications intermediaries or one's own system may intercept messages to protect the recipient from malware or unsolicited commercial messages. The law does not put the risk of loss of messages for that reason on the operator of the filters, for critical information like the start of a legal action.¹⁸³

There are two important exceptions to this rule. The general insistence on personal service applies to the first attempt to serve. If the party cannot be found, or appears to be evading service, then the party trying to start the proceeding may apply to the court for permission to use other methods.¹⁸⁴ These have traditionally included publication in newspapers, service on another person likely to pass on the document to the addressee, and other such methods. A handful of cases in common-law countries, none apparently in Canada to date, have been prepared to extend such 'substitute service' to electronic means. Some US courts have permitted service by email, if the address could be justified.¹⁸⁵ An Australian court has allowed substitute service to a mobile phone.¹⁸⁶ Recently an Australian court

182 UN Model Law on Electronic Commerce, above note 24, article 15, Uniform Electronic Commerce Act, above note 43, s. 22, *Electronic Commerce Act, 2000*, S.O. 2000 c. 17 s. 22(3).

183 A good argument can be made that in normal commercial communications between equally sophisticated parties, each party should bear the risk of an over-exclusive filter. That risk can also be allocated by contract, but not for the purposes of starting a legal proceeding.

184 See Ontario Rules of Civil Procedure, Rule 16.04.

185 *Rio Properties v Rio International Interlink*, 284 F.3d 1007 (9th Cir. 2002).

186 *NRL v Sonny Bill Williams*, reported in *The Age* (Australia), August 5, 2008, online: <http://news.theage.com.au/sport/bulldogs-get-one-up-on-sonny-bill-20080805-3q43.html>.

authorized a plaintiff to serve the defendants by sending the notice to their Facebook site.¹⁸⁷ In that case, the plaintiff had spent substantial efforts to locate the defendants by traditional means, including by private detective, and there was strong evidence that the Facebook site was duly linked to the targeted defendants. A New Zealand court has done the same.¹⁸⁸ These cases will depend on their own facts for some time before any rule can be formulated.

The other exception on e-service is for documents to be served after the litigation is started. Ontario requires for this purpose that the parties all be represented by lawyers – no e-service on a self-represented litigant, therefore – and that the lawyers consent to service in that way.¹⁸⁹ Further, receipt of the electronic service must be confirmed by the addressee for it to be effective.¹⁹⁰ In other words, once all parties are paying attention, they may agree to use electronic communications, and even then the Rules provide limits.¹⁹¹

One international development may be of interest. In February 2009, The Hague Conference on Private International Law held a special meeting of parties to its Convention on Service Abroad of Documents in Civil and Commercial Matters.¹⁹² The questionnaire circulated to the parties before the meeting asked if they permitted electronic service under their domestic law. The replies suggested that only a few countries had modified their law to accommodate new technologies, and there have been few actual cases of their use, usually as a last resort.¹⁹³ So different court systems are moving only very cautiously to electronic service.

(b) Filing

Once the document is served, can it be got to the court electronically? The advantages of electronic records are widely recognized, within as well as outside the court offices: speed and economy of transmission, ease of management and retrieval, ability to back up to avoid loss, reproducibility for all required users. The disadvantages are also appreciated: doubts about authentication (once again), concerns about continued integrity of the document, risk of loss despite backups.

Electronic filing is coming, at a different pace in different places. The Supreme Court of Canada insists on having electronic versions of pleadings,¹⁹⁴ as does the Ontario Court of Appeal, which extends the

187 The Sydney Herald, December 12, 2008, online: <http://www.smh.com.au/news/technology/web/australian-court-serves-documents-via-facebook/2008/12/12/1228585107578.html>. The message was required to be sent 'privately', rather than posted on the wall where everyone could see it.

188 *Ace Market Gardens v Axe*, High Court. Reported in the New Zealand Herald, March 16, 2009. Online: http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10561970.

189 See Ontario Rules of Civil Procedure, Rule 16.05(1)(f).

190 *Ibid.* See also Rule 16.09(6)(a) on Proof of Service.

191 The American Bar Association, Section of Science and Technology, had a committee develop principles for electronic service. Its “Best Practices for Electronic Service of Process” (2006) are online: http://meetings.abanet.org/webupload/commupload/ST230005/otherlinks_files/2006-01-23_AdoptedRevisedBP.pdf. U.S. legal principles are sufficiently close to ours on such matters that the results are of interest here too.

192 Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, online: http://www.hcch.net/index_en.php?act=conventions.pdf&cid=17.

193 Conclusion and Recommendations of the Special Commission on the Practical Operation of The Hague Apostille, Service, Evidence and Access to Justice Conventions, 2 – 12 February 2009, online: http://www.hcch.net/upload/wop/jac_concl_e.pdf, para.38..

194 The Supreme Court of Canada rules and forms are described online: <http://www.scc-csc.gc.ca/ef-de/index-eng.asp>

same demand to the appeal book.¹⁹⁵ British Columbia now has widespread electronic filing in its Supreme Court too.¹⁹⁶ Several American jurisdictions have e-filing, including all the federal bankruptcy courts in the country.¹⁹⁷ In many of these jurisdictions, e-filing is not only permitted but mandatory.

Ontario ran two pilot projects for e-filing in the Superior Court, one of them extending as well to the Small Claims Court. One depended on filing word-processed documents as attachments to an email filing, the other was web-based and dealt with pleadings in Portable Document Format (PDF). Both were supported by Rules of Civil Procedure.¹⁹⁸ The Ontario rules allowed for electronic filing of affidavits of service and other documents that needed a signature by what was referred to above as the “outsourcing” method. The party filing the document would add an electronic certificate that the signed paper was in that party’s possession. Any failure to produce the paper on request was subject to sanctions up to and including dismissal of one’s side of the case.¹⁹⁹

These projects never got beyond electronic filing of pleadings that were then printed out by the court office for use by judges. It was intended that the court office would go electronic in due course. When that prospect receded dramatically, the pilot projects were discontinued.²⁰⁰ Both projects relied on the use of software provided by the government, in a version approved by the judiciary. All participants were authenticated. Only lawyers were allowed to use the system. While the pilot projects proved popular with the Bar, they left a number of issues unresolved. For example:

- How can the technology be made accessible to all litigants economically? Individual PKI licences for members of law firms can be more expensive than using paper filing. Unrepresented litigants will have little need for a full licence but a great need for dedicated training on how to use the technology that lawyers will learn as part of their practices.
- How can the filed information be kept secure from tampering, degradation or prying eyes? How much security is appropriate – more than currently applied to the paper files? The general question of access to electronic court records has created considerable debate, including policy reviews by the Canadian Judicial Council²⁰¹ and both federal²⁰² and state courts²⁰³ in the United States.

195 The Ontario Court of Appeal rules and forms are described online:

<http://www.ontariocourts.on.ca/coa/en/notices/adminadv/ef.htm>.

196 The British Columbia courts' e-filing system is described online: <https://eservice.ag.gov.bc.ca/cso/index.do>. E-filers must have an agreement with the Courts to participate; in other words, it is a closed system. Users are authenticated by a user ID and password, but the user agreement gives the Courts the right to use a more secure signature system. The agreement is online: <https://eservice.ag.gov.bc.ca/cso/usageAgreement/index.do> para. 13-14.

197 All U.S. Bankruptcy courts have e-filing rules. For example, California's are online:

<http://www.canb.uscourts.gov/procedures/dist/electronic-case-filing-procedures>.

198 See for example O.Reg. 427/01 for the principal amendments supporting web-based e-filing. The applicable rules were revoked by O.Reg. 14/04.

199 Another example of this technique is described above TAN105.

200 The projects both became part of the government's “Integrated Justice Project”. The project was unable to deliver the court office system for reasons beyond the scope of this paper.

201 Canadian Judicial Council, “Open Courts, Electronic Access to Court Records, and Privacy” (2003), online: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_OpenCourts_20030904_en.pdf. A synthesis of replies is also online: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Synthesis_2005_en.pdf.

202 The current federal judicial privacy policy is online:

http://www.privacy.uscourts.gov/privacypolicy_Mar2008Revised.htm. Some of the policy issues are outlined in a 2007 request for comments on elements of the policy, online: <http://www.privacy.uscourts.gov/requestcomment.htm>.

203 Resources provided by the National Center for State Courts are online:

- How can non-expert counsel and judges make informed decisions about what technology is acceptable? The integrity of the system is crucial for all, and the judges have particular responsibility for it. Can the same advice be available for all participants?
- How can technical standards be maintained in a fast-evolving field? The earlier discussion of authentication²⁰⁴ noted that such systems tend to be closed, depending on all participants using prescribed technology – but prescribing means fixing, to some extent, in an evolving field.
- How can compatible rules be maintained across all judicial if not legal uses, while maintaining appropriate controls on each court’s system, and appropriate protections for the privacy of the information in the records?²⁰⁵

While electronic filing is probably inevitable, it will not soon be universal.

(c) Trials

Trials themselves are still being held in person, though applications for leave to appeal to the Supreme Court of Canada, and occasional arguments on appeal, have been heard by videoconference. Administrative tribunals in Ontario can make rules to govern their electronic hearings.²⁰⁶ Private online dispute resolution was discussed briefly earlier in this article.²⁰⁷ The broadcast of court proceedings is a separate question entirely – though an Ontario court recently gave a reporter the right to sent Twitter messages directly from the courtroom during trial.²⁰⁸

An interesting new phenomenon arising from increasingly mobile communications is the communication of proceedings from the courtroom by participants, not observers. In an Arkansas civil case a juror sent Twitter messages during deliberations, including one that said “I just gave away TWELVE MILLION DOLLARS of somebody else’s money.” The court dismissed a motion for a mistrial, though it was critical of the practice.²⁰⁹

Jurors have commented on trials during cases in blogs and Twitter postings, as well. One juror in a high-profile criminal case even sent a Twitter teaser, “Stay tuned for a big announcement Monday.” Here too the court refused to take the case from the jury.²¹⁰

Jurors have proved themselves inclined to research the cases they are hearing, given the ease of access of search engines. In early 2009, a juror in a Florida drug trial admitted to the judge that he had been

<http://www.ncsconline.org/WC/CourTopics/ResourceGuide.asp?topic=PriPub>.

204 Above, TAN 102.

205 For a fuller discussion, see J.D. Gregory, “Electronic Filing in Ontario: Practices and Policies”, (2004) 4 E-Filing Report No. 4 p. 1, online <http://www.euclid.ca/efiling2004.htm>.

206 *Statutory Powers Procedure Act*, R.S.O. 1990 c. S.22, s. 5.2 and 5.2.1

207 Above, note 125.

208 D. Butler, “Judge allows live reporting from inside courtroom”, Ottawa Citizen, May 5, 2009. The same ruling was made for a long trial in London, Ontario, in the spring of 2009, and in Kansas earlier in 2009: L. Marek, “Twitter has a Voice in Federal Court”, LTN Law Technology News, March 16, 2009, online: <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202429062432&slreturn=1&hbxlogin=1>.

209 M. Neil, “Juror Tweets in \$12.6M Case Teach Lawyer a Lesson: Ask About Web Use”, ABA Journal, April 6, 2009, online:

http://www.abajournal.com/news/sweet_news_for_plaintiff_in_12.6m_case_jurors_tweets_wont_change_verdict

210 S. Duffy, “Federal Jury Finds Former Pa. State Sen. Vincent P Fumo Guilty on All Counts”, Law.Com, March 16, 2009, online: <http://www.law.com/jsp/article.jsp?id=1202429098920>.(paywall)

doing research online on the case, despite the judge's instructions. The judge inquired of the other jurors, and it turned out that a majority had done so. He declared a mistrial, eight weeks into a trial.²¹¹

In another Florida case, a witness engaged in text-messaging while he was on the stand, during a break when the judge was conferring with the attorneys. The judge declared a mistrial.²¹²

The Southern District of Florida has made an administrative order saying "emailing, text messaging, twittering, typing, and using cellular phones shall continue to be prohibited inside the District's courtrooms." However, journalists could bring into courtrooms "cellular phones, Blackberries, iPhones, Palm Pilots, and other similar electronic personal digital assistants (PDAs) into the courthouse consistent with what is permitted of attorneys, as long as the news reporters agree in writing not to email, text message, twitter, type, or use their cellular phones or other electronic device inside the District's courtrooms."²¹³

2. Electronic Discovery

Once the documents are served and filed, the next stage in normal litigation is examination for discovery. Part of that process is the disclosure of relevant documents by each party. Rule 30 of Ontario's Rules of Civil Procedure²¹⁴ has long been drafted in media-neutral terms. Its present form defines "document" to include (so it is not limited to) "a sound recording, videotape, film, photograph, chart, graph, map, plan, survey, book of account, and data and information in electronic form."

(a) E-discovery in general

It has become apparent to litigators and courts in the past few years that the proliferation of electronic records and the equally rapid diversification of electronic storage media present a serious challenge to litigants. How can they find everything they have that is relevant, and how can they hope to analyse everything that the other party may disclose? Moreover one needs to analyse one's own material, not just for relevance but for reasons not to disclose it, such as solicitor-client privilege.²¹⁵ Finding the information across so many information systems can be prohibitively expensive. Who pays for it? How much time is allowed?

The courts have begun to address these issues, especially in the United States. The leading case is the *Zubulake* decision, in five parts!²¹⁶ It established a number of practices and principles that have

211 J. Schwartz, "As Jurors Turn to the Web, Mistrials Are Popping Up", New York Times, March 17, 2009, online: http://www.nytimes.com/2009/03/18/us/18juries.html?_r=1.

212 A. Roberts, "Mistrial Declared Over Executive's Texting From Witness Stand", Daily Business Review, May 15, 2009, online: <http://www.law.com/jsp/article.jsp?id=1202430721257> (paywall)

213 S.D. Fla. Admin.Order 2009-12, online: <http://www.flsd.uscourts.gov/wp-content/uploads/2010/07/2009-12Prohibition-on-Electronic-Transmissions-and-Cellular-Phone-Use-Inside-Courtrooms.pdf>. Compare that direction with the order of the Kansas court referred to in footnote 204 above. Is this the first court practice direction to mention twittering?

214 R.R.O. 1990 c.194 as (frequently) amended.

215 For an example of how hard – and expensive – that can be, see *Air Canada v. Westjet Airlines Ltd.*, (2006), 81 O.R. (3d) 48 (Sup.Ct.) The prospect of having to do the costly triage of its records to find those subject to privilege in its favour helped move Air Canada to settle the case, though it was plaintiff and the purported aggrieved party.

216 *Zubulake v UBS Warburg LLC*: I: 217 F.R.D. 309 (SDNY 2003), addressing the cost standard for producing emails from backup tapes; II:2003 WL2108730 (SDNY May 2003), addressing *Zubulake's* reporting obligations; III: 216

become accepted in that country and here: the lawyers should meet and confer about the scope and method of electronic discovery; e-discovery should be proportionate to the importance of the issues and amounts in litigation; parties should bear their own costs, but courts may vary that rule in appropriate circumstances.²¹⁷ Subsequent courts have set out rules about how electronic records are to be preserved for discovery, and have sanctioned heavily parties who have failed to produce full information or who have pre-emptively destroyed some of it.²¹⁸ The law of spoliation of evidence has had a major revival thanks to e-discovery cases.²¹⁹

Bench and Bar in the US sought out technical assistance and put together some informal but very influential guidelines known as the Sedona Principles²²⁰ largely based on the jurisprudence but providing further details for its general implementation. Canadian lawyers and judges picked up on this idea and adapted those principles to create the Sedona Canada Principles.²²¹ Ontario has amended its Rules of Civil Procedure to provide for processes and principles similar to the Sedona recommendations.²²²

The issues in electronic discovery are complex and in rapid evolution. The topic has been reviewed in a recent previous edition of this publication.²²³ A number of comprehensive guides are available, and readers are directed to them for more details.²²⁴

(b) E-Discovery and privacy

The obligation of a party to disclose information to the other side in a civil action is subject to a few limitations, notably that of solicitor-client privilege.²²⁵ Likewise there are limitations on the use one may make of the information. A deemed undertaking restricts use to matters relevant to the action in which the discovery is made.²²⁶ The privacy rights of the disclosing party are not expressly mentioned in the rule but are a core principle behind it.²²⁷ The way that electronic communications may play a

F.R.D.280 (SDNY 2003), allocating backup tape restoration costs; IV: 220 F.R.D. 212 (2003), ordering sanctions against UBS Warburg for failure to preserve evidence; V: 2004 WL 1620866 (July 20, 2004), addressing further sanctions against UBS Warburg and its counsel for failure to produce emails.

217 The costs rule varies in the US, where parties generally bear their own costs. Canadian courts can compensate the winning party for some part of its costs in any event.

218 *Coleman v Morgan Stanley*, 2005 WL 679071 (Fla. Cir. Ct. March 1, 2005).

219 See *McDougall v Black & Decker Canada Inc.*, 2008 ABCA 353. On record retention and destruction policies in the light of e-discovery, see D. Michaluk, "A lawyer's perspective on records retention and destruction", May 2009, online: http://danmichaluk.files.wordpress.com/2009/05/paper_lawyeronrm_may28-085835.pdf.

220 For a selection of relevant publications of the Sedona Conference, see online: <http://www.thesedonaconference.org/publications.html?grp=wgs110>.

221 Online at: <http://bit.ly/oeu2Zq> (printfu.com).

222 See O.Reg. 438/08 for the collection of rules, most of which come into force on January 1, 2010. See in particular Rule 29.1.03(4).

223 D. Urbas, "Spoliation and Electronic Documents: Putting the Spark back into Discover", [2006] *Annual Review of Civil Litigation* (Carswell: Toronto, 2006), page 279..

224 Collections of sources are frequently updated by LawPRO (the Lawyers' Professional Indemnity Company of Ontario), online: <http://www.practicepro.ca/information/default.asp?ename=ED#ED> and its reading list at: http://www.practicepro.ca/practice/eDiscovery_Rlist.asp; and by the Ontario Bar Association, online: http://oba.org/en/publicaffairs_en/e-discovery/default.aspx.

225 Ontario Rules of Civil Procedure, Rule 30.02(2).

226 Ontario Rules of Civil Procedure, Rule 30.1.01(3)

227 *Kitchenham v. AXA Insurance Canada*, (2009), 94 O.R. (3d) 276, (C.A.) at 278, para [1]: "...interference with that privacy interest is justified ...".

role in making personal information available has inspired several facets of litigation.

The apparent anonymity of people online has created problems for those who feel aggrieved by the online actions of such people. Accordingly a number of courts have been asked to compel Internet Service Providers to disclose the names and addresses of alleged wrongdoers, who may be hidden behind a pseudonym. One of the leading cases is *BMG Canada Inc. v John Doe*.²²⁸ There the Federal Court of Appeal upheld a refusal to compel disclosure of the names of people who had allegedly shared music files online. The Court said that privacy rights were not absolute, but the court had to balance them against the demands of justice in the case.

A case in early 2009 contrasted privacy and free speech rights with the enforcement of human rights. The plaintiff wanted to stop anti-Semitic defamation by people commenting in a 'chat' section of a right-wing web site. The site owners submitted that anonymous posters had an expectation of privacy and that the plaintiff should have to show at least a prima facie case of liability before being given the names. The court held that the names must be disclosed because the Rules, especially Ontario's Simplified Rules, require parties to disclose all relevant documents, including lists of names.²²⁹

The amount of information one keeps in electronic form and the ease with which it may be searched may make normal discovery practices overly intrusive. An application to order discovery of a party's hard drives, including the metadata associated with the records, and the party's history of sites visited with her browser, was refused on the ground that it included too much necessarily irrelevant material. A more focused request was required.²³⁰

However, the expectation of privacy created by online privacy policies are not a barrier to disclosure for litigation purposes. A few examples will illustrate:

- A plaintiff in a personal injury case was not allowed to protect the 'private' status of her Facebook pages that showed her physically active. The court noted that her private pages were shared with numerous 'friends', and thus the claim of confidentiality was not credible.²³¹ It is clear that Facebook pages are 'documents' subject to discovery under the Rules.
- However, it has been ruled unethical for a lawyer to have someone ask a party to a lawsuit to make that person their "friend" on the party's social networking site, in order to get access to private

228 [2004] CanLII FC 488, [2004] 3 F.C.R. 241, affirmed [2005] CanLII CAF 193, [2005] 4 F.C.R. 81 (C.A.).

229 *Warman v Wilkins-Fournier*, [2009] CanLII 14054 (ON S.C.). The court distinguished the *BMG Canada* case on the grounds that different Rules were applicable and different claims were made in the case. The case may be subject to appeal. Many US cases have required a heightened evidentiary standard before compelling ISPs to disclose the identity of anonymous users. The decision was reversed on appeal by the Divisional Court on May 3, 2010, and remanded for reconsideration. The reconsideration came to the same result as the first court:
<http://www.canlii.org/en/on/onsc/doc/2011/2011onsc3023/2011onsc3023.html>.

230 *Desgagne v Yuen* 2006 BCSC 955.

231 *Murphy v Perger* [2007] OJ No.5511 (S.C.J.). In *Leduc v Roman*, 2009 CanLII 6838 (ON S.C.) the court held that it was irrelevant whether the discoverable documents were on private or public pages, so long as they were relevant to the case. Other Canadian social networking cases are mentioned at paragraphs 23 of the *Leduc* decision. A request for photographs on Facebook and MySpace was refused when it too close to trial, could have been made earlier (since photographs were clearly documents subject to discovery) and would involve significant time to sort for privacy interests of third parties. *Kent v Laverdière*, 2009 CanLii 26741 (ON S.C.). See P. D. Pengelly, "Fessing Up to Facebook: Recent Trends in the Use of Social Network Websites for Insurance Litigation", March 23, 2009, Available at SSRN, online: <http://ssrn.com/abstract=1352670>.

information outside the discovery process.²³²

- Someone who posted derogatory comments about her community on MySpace had no legal complaint when these comments were republished in a community paper, leading to intense negative pressure on her that drove her out of town.²³³
- The right of employers to get access to employees' off-hours MySpace postings and fire them for their criticisms of the employer are at issue in a New Jersey case that will test whether one has any expectation of privacy for what is on the Internet, even behind a password.²³⁴

The law is in evolution along with the technology, but the broad limits of discovery seem likely to be maintained against electronic barriers to disclosure.²³⁵

3. Electronic Evidence

Once one has found the relevant electronic information, whether in one's own files, from one's own witnesses, or on discovery from the other side, one needs to be assured that it is admissible in court. What the judge makes of the admitted evidence is a matter of weight, which may involve rearguing some of the reliability points that affect admissibility as well.

(a) Admissibility in general

Are electronic documents reliable enough to be admitted in evidence? What supporting or foundational evidence needs to be presented to ensure their admission? These questions occupied the Ontario Court of Appeal in the late 1970s in *R. v McMullen*,²³⁶ a case about banking records. The court found that extensive background information was required, to show how the records had been kept and how produced in court.

The nature and quality of the evidence put before the Court has to reflect the facts of the complete record keeping process – in the case of computer records, the procedure and processes relating to the input of entries, storage of information, and its retrieval and presentation. ... If such evidence be beyond the ken of the manager, accountant or the officer responsible for the records ... then ... the print-out evidence would be inadmissible.²³⁷

232 Philadelphia Bar Association Professional Guidance Committee, Opinion 2009-02 (March 2009), online: <http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion2009-2.pdf>.

233 *Moreno v Hartford Sentinel*, Cal. C.A. 2009, described in M. McKee, "MySpace Musings Aren't Private, Appeals Court Rules", Law.Com, April 6, 2009, online: <http://www.law.com/jsp/article.jsp?id=1202429677896>. (paywall)

234 D. Searcey, "Employers Watching Employees Online Spurs Privacy Debate", Wall Street Journal April 23, 2009, online: <http://online.wsj.com/article/SB124045009224646091.html>.

235 A debate has arisen in criminal cases whether the police should need a warrant to compel ISPs to disclose the names and addresses behind IP addresses. Are these no different from the names and addresses routinely found in a telephone directory, or does the potential to combine them with the content of communications made from those addresses give their divulgence much more potential to incriminate the people so named? Recent cases in Ontario at least have suggested some division, but there may be a trend to easier disclosure. A summary of some of the cases is in E. Baum, "On the Internet, nobody knows you're a ...", The Court blog, March 31, 2009, online: <http://www.thecourt.ca/2009/03/31/when-youre-online-no-one-knows-youre-a/> Some of this reasoning may spill over into civil discovery as well.

236 (1979), 100 D.L.R. (3d) 671, 47 C.C.C.(2d) 499.

237 *Ibid.*, p. 506 (C.C.C.)

However, the Supreme Court of Canada held a few years later that for business and banking records, if the owner of the records relied on the records in the normal course of business, then the records should be considered reliable enough to be admitted in court.²³⁸ As a consequence, Canadian courts have not had great difficulty admitting electronic records.

One needs to take care in using the word “reliable”, since can be applied casually, or generically, to mean that records have not been altered, but reliability is also used as a key test for the admissibility of hearsay evidence. It is arguable that the courts have not clearly separated out hearsay questions from questions of authenticity. Electronic documents do not in principle present more questions of hearsay than documents on paper.²³⁹ They either are or are not a reliable (in the sense of accurate) record of the information in them. Many e-documents presented in court cases are business records, and the normal business records rules can safely apply to them.²⁴⁰ So questions whether the information has been accurately recorded by someone knowledgeable of the facts can be answered the same way for electronic as for paper records.²⁴¹

This does not necessarily ensure that the records are what they purport to be, a different question. Two American cases have attracted attention on that topic. In the first, *In re Vee Vinhee*,²⁴² the court refused to accept American Express’s records on what the defendant owed, being unpersuaded by the plaintiff’s expert that the records were accurate. American Express lost its collection case even though the defendant did not show up. The judge’s questions can be a useful checklist of what one needs to be able to support if the records are put in issue.

[T]he focus is not on the ... creation of the record, but rather on the ... preservation of the record during the time it is in the file.

[T]he entity’s policies and procedures for the use of the equipment, database and programs are important. How access to the ... database [and to the specific programs are] controlled is important. How changes in the database are logged, as well as the structure and implementation of backup systems and audit procedures for assuring the continued integrity of the database, are pertinent.²⁴³

238 *R. v. Bell and Bruce*, (1982), 35 O.R. (2d) 164 (C.A.), affd [1985] 2 S.C.R. 287. One may ask whether this principle should be readily extended beyond banks, which are strictly regulated, to any business, or any record holder. For a policy analysis of the differences between these two cases, see H. Stewart, “Electronic Evidence”, [1996] Proceedings of the Uniform Law Conference of Canada, online: <http://www.ulcc.ca/en/poam2/index.cfm?sec=1996&sub-1996aa>.

239 Electronic documents may often be produced for reasons other than to prove the truth of their contents – such as to show that a statement was made or an action taken by someone at a particular time – and these do not raise hearsay questions at all.

240 The Ontario *Evidence Act*, R.S.O. c. E.23, includes electronic records in its codification of the business records exception to the hearsay rule. S. 35(1): “‘Record’ includes any information that is recorded or stored by means of any device.”

241 One experienced Canadian authority takes the view that e-records raise new hearsay questions as well. See K. Chasse, “Electronic Records as Documentary Evidence”, (2007), 6 Can.Jl. of Law and Technology No. 3 p. 141. He refers to “the faulty concept that computer software neatly and clearly separates its issues of fact and law into hearsay rule and best evidence rule varieties. In fact, electronic record systems irretrievably scramble them together.” (p. 145)

242 *In re Vin Vinhee*, 336 B.R. 437 (Bkcy, 9th Cir. 2005)

243 *Ibid.* Some of the language here and in the following case recalls that of the Ontario Court of Appeal in *McMullin*, above note 237.

The other case, *Lorraine v Markel*,²⁴⁴ involved a motion for judgment that tendered printouts of emails as evidence. These documents should have been submitted under oath, as in an affidavit. The judge took the opportunity to provide a nearly 100 pages on the frailty of electronic records and what should be done to support them. In most cases this technological support will not be necessary, and having to provide it in every case with electronic records would cripple litigation with the expense. In most cases the authenticity of the e-documents is not contested. However, again the case can be a checklist for lawyers of the kinds of issues that can come up, or of challenges that one might make to the other side.

For example, one may need testimony of a witness who describes specifically the process by which the electronically stored information is created, acquired, maintained and preserved without alteration or the process by which it is produced. The possibility that the evidence has been changed by the search and collection itself must be guarded against. In some cases one may be able to authenticate a record by circumstantial evidence, including its own contents. Other techniques are described in the decision, some more focused on U.S. Rules, others possibly applicable in Canada as well.²⁴⁵

Many jurisdictions have a “notice to admit” process, which involves disclosing to the other party before trial the documents one is going to rely on. If there is no objection within a specified time, then the documents are admitted without challenge.²⁴⁶ Using this procedure for electronic documents can save time and cost of technical disputes.

It is clear from the two cases mentioned, and from the discussion of electronic discovery in the last section, that the proper creation and management of electronic records is crucial to one’s capacity to advance one’s legal interests in the courts. The Canadian General Standards Board has adopted a Standard for the Admissibility of Electronic Records as Documentary Evidence.²⁴⁷ Proof of compliance with the Standard would be a serious support for admission of the documents to be produced.

The essence of the CGSB Standard is to make a defensible record management policy, educate people about it (a policy manual is essential), and monitor compliance with it (including ensuring that audit trails are available for all important information.). The policy should deal with, among other things, data file formats and version control, enabling technologies, quality assurance, metadata capture and preservation, the physical and logical structure of information held by the organization, and security classifications and processes and their implementation. Record retention and destruction schedules play a role too. Finally, someone should be available to testify knowledgeably about all of these elements.²⁴⁸ In short, have a careful policy and be able to show that you adhered to it. This will be helpful to support both electronic discovery and the subsequent admission of relevant evidence at trial.

244 *Lorraine v Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007)

245 A useful summary of the discussion in the *Lorraine* decision is found in “*Lorraine v Markel*: Electronic Evidence 101”, online: http://www.lexisnexis.com/applieddiscovery/LawLibrary/whitePapers/ADI_WP_LorraineVMarkel.pdf.

246 See for example Ontario’s Rules of Civil Procedure, Rule 51. Compare American Federal Rules of Civil Procedure 26.

247 Canadian General Standards Board, *Electronic Records as Documentary Evidence*, CAN/CGSB-72.34-2005, described online: http://www.techstreet.com/cgi-bin/detail?doc_no=can_cgsb/72_34_2005;product_id=1252845. A quick overview can be found in a slide deck by J.D. Gregory, “Electronic Records and the Law” (March 2007), online: <http://www.verney.ca/opsim2007/presentations/301.ppt>.

248 The American Bar Association has also published a set of best practices for record retention and destruction.. *Record Retention and Destruction: Current Best Practices* (2003), online: <http://apps.americanbar.org/buslaw/newsletter/0019/materials/recordretention.pdf>.

(b) The best evidence rule

A particular problem in admitting electronic evidence is the “best evidence rule”. This common law rule requires parties to tender the best evidence available in support of their arguments. For documents, this has meant that one must tender an original document rather than a copy, or give good reasons why an original is not available. Originals are considered harder to alter undetectably than copies. They may also be easier to read, though that is more of an issue for carbon-paper copies than photocopies.

The challenge for electronic documents is that it is hard to say what the original is. Further, digital copies are perfect copies: all the ones and zeroes, the bits and bytes, are reproduced exactly. The “original” is no better than the “copy”. One can be altered as readily and as undetectably as the other. Thus the best evidence rule makes little sense when applied to electronic records.

This issue has been resolved by legislation in most Canadian jurisdictions. The Uniform Electronic Evidence Act²⁴⁹ has been adopted in six provinces, the Yukon territory and federally.²⁵⁰ It provides that the best evidence rule can be satisfied for an electronic record by proof of the integrity of the electronic record system from which it comes. The principle is that without an authoritative “original” to compare it with, the integrity of an electronic document cannot be proved directly. (If one had a live witness under oath capable of testifying to the information in the document, one would not need the document at all.) Thus system integrity is a substitute for individual document integrity. The Uniform Act provides some presumptions of integrity as well, to avoid costly foundation evidence where there should be no dispute.

The first presumption is that records from the proponent’s own computer are reliable if the systems are shown to have worked properly during the relevant period, or if not, that the problems were not pertinent to the information being presented to the court. Second, documents received from an adverse party are presumed reliable; it is up to the owner of the system from which they came to show their unreliability if that is alleged.²⁵¹ Third, documents from a third party that created them in the ordinary course of business, not subject to the control of the party seeking to produce them in court, are also presumed reliable.²⁵²

If these presumptions do not apply or are rebutted, the parties must show the integrity of the record system in some other way. The Uniform Act expressly authorizes courts to consider if the record-keeping system was maintained according to accepted standards. This would give the proponent of electronic evidence the opportunity, for example, to demonstrate compliance with the Canadian General Standard Board rules mentioned in the previous section. Adherence to a standard does not guarantee admissibility, but it would be a significant support for it. Private standards of a particular industry would be relevant for this purpose, or even standards agreed on by parties to a contract.²⁵³

249 Uniform Electronic Evidence Act, [1998] Proceedings of the Uniform Law Conference of Canada p. 164.

250 See the Uniform Law Conference’s chart of implementation online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4b>. The legislation is discussed in more detail in J.D. Gregory, “Canadian Electronic Commerce Legislation”, above note 41, at pp. 326 - 338.

251 Compare *Indianapolis Minority Contractor Assn v Wiley*, 1998 U.S. Dist. LEXIS 23349 (D.Ind. May 13, 1998), holding that a party cannot produce information in discovery and then claim that the opposing party must authenticate it.

252 Uniform Electronic Evidence Act, above note 249, s. 5. Compare Ontario Evidence Act, s. 34.1(7).

253 This provision was in part intended to answer the concern expressed in the Uniform Law Conference consultations

Though the Uniform Act is written with a view to replacing the best evidence rule, it seems both likely and appropriate that the support it develops for the reliability of an electronic record-keeping system could apply to questions of authentication as well,²⁵⁴ and arguably of reliability for the purposes of the hearsay rule.

Two technical notes are needed to close out this part of the discussion.

First, we are talking here about proving the content of a record as a record. If the electronic evidence purports to show something else, different rules may apply. In particular, an analysis of data using a special program to detect fraud may be expert evidence, not a business record, and it should be supported by qualifying its author as an expert in the usual way.²⁵⁵ Computer-generated re-enactments of events at issue in litigation would be subject to similar considerations beyond the scope of this paper.

Second, the Uniform Act defines electronic record to include a printout. That is because the printout is used to demonstrate the contents of the computer, just as a display on a monitor may do. The printout is no more reliable as a source of the information than the electronic data in the computer, so it is subject to the same rules as other electronic data. However, sometimes a printout can become the only relevant record. Business correspondence these days is invariably generated by a word-processing program, but it is often tendered in evidence not to show the contents of the originating computer but to show what information was communicated on paper from one person to another at what time. A printed and mailed invoice may be the same. In this case the Uniform Act provides that such a record should be treated as a paper document for the purposes of the best evidence rule.²⁵⁶

(c) Metadata

Metadata are data about data. In particular they are data generated automatically by the software used to create the document, or by the system on which it is created, that may reveal when the document was created and by whom and that may show changes from one version to the next and who made the changes, and also when and to whom the document was transmitted. Different software and systems have different capabilities. Photographs may also contain metadata, about the time they were created and the type of camera, among other data.²⁵⁷

These data are very useful to the creator of the document. The UN Model Law on Electronic

that private parties may not be able by contract to waive the rules of evidence.

254 Canadian case law has not consistently analysed admissibility issues into authentication and best evidence elements. The principle of the Uniform Act was that the reliability of the evidence should be determined once, not twice, and that should be done within the best evidence rule. Authentication was left to any evidence capable of supporting that the record was what it purported to be, and that test was not necessarily demanding. The evolution of case law especially in the United States since the Uniform Act was adopted in 1998 has put the weight of the question on authentication not best evidence.

255 See for example *R. v. George*, [1993] A.J. No.798 (AB Prov Ct).

256 Uniform Electronic Evidence Act, above note 249, section 4(2). Unfortunately the version of this exception in the *Canada Evidence Act*, R.S.C. 1985 c.C.5, s. 31.1(2), says instead that the printout in these cases *is* the best evidence, rather than just that it is subject to the traditional best evidence rule so the (paper) original should be produced.

257 D.Johnson, "Protect Your Privacy When Uploading Photos", PC World April 9, 2009, online: http://www.pcworld.com/article/161775/protect_your_privacy_when_uploading_photos.html and "Hidden Data in JPEG Files", (2009) Word Investor, online:<http://wordinvestor.blogspot.com/2009/11/hidden-data-in-jpeg-files.html>.

Commerce and its Canadian implementing legislation²⁵⁸ say in their rule about the retention of electronic records that the information to be kept should include information about the origin, destination and time of transmission of a document that was sent to the record keeper.²⁵⁹ The same principle can readily be applied to metadata generally. Their absence from the uniform rule just shows that people were less sensitive to the scope of metadata generally when the rules were formulated.

However, metadata can also be very useful to someone adverse in interest to the creator.²⁶⁰ As a result, litigators requesting discovery of documents increasingly ask for the documents in their “native format”, meaning in the electronic format that will reveal the metadata, and courts are requiring compliance.²⁶¹

Likewise solicitors exchanging documents electronically during negotiations of deals are learning to be careful about the content of those documents. Methods are available to reduce or eliminate metadata from documents, though it may be inappropriate to use such methods if the documents are likely to be needed for litigation.

If documents are disclosed that unintentionally include metadata, are the recipients entitled legally or ethically to read them? Legally, all information that is disclosed can be used.²⁶² The courts have not protected metadata as they have sometimes protected privileged documents, though one cannot count on having privilege protected if one is negligent in disclosing it. Ethics opinions have differed. The current Canadian position is that someone receiving unintended disclosure of metadata can look at it.²⁶³ The majority American position is the same,²⁶⁴ but some state bar associations have taken the opposite view.²⁶⁵ These days, questions of metadata are prominent enough that any unintended disclosure would probably raise questions of professional negligence.

(d) Some special cases

Courts have taken different views on whether information on web sites is reliable enough to be admitted in evidence. If the content of a web site is to be introduced to show its truth, then one must

258 See the discussion above, TAN 43 – 61.

259 See UECA s. 13.

260 D. Pinnington, “Beware the Dangers of Metadata”, Law Pro magazine, June 2004, online: <http://www.practicepro.ca/LawPROMag/metadata.pdf>

261 See T. Baldas, “Metadata Grows in Legal Import”, National Law Journal, January 26, 2009, online at LTN Law Technology News: <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202427709683>. The article cites a number of recent cases.

262 *Prism Hospital Software Inc. v. Hospital Medical Records Institute*, [1991] BCJ No. 3732 (BC SC) – information restored from deleted backup tapes was admissible and was not an expression of expert evidence.

263 The Canadian Bar Association, *Guidelines for Practising Ethically with New Information Technologies*, online: <http://www.cba.org/CBA/activities/pdf/guidelines-eng.pdf>, p. 11, warns the sending lawyer to get rid of metadata, but says nothing about any duty on the recipient to refrain from mining the data. Technical issues are discussed at pp. 24 – 28.

264 American Bar Association, Formal Opinion 06-442 (August 5, 2006)

265 For example, New York State Bar Opinion 782 (2003) bars use of metadata disclosed inadvertently, and Opinion 749 speaks strongly against the use of special tools to find metadata not ordinarily accessible. Florida Bar Opinion 06-2 (September 15, 2006) takes the same view. A chart of ethics opinions on metadata appears at the ABA Legal Technology Resource Center, online: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatar.html.

meet the rules for admitting hearsay.²⁶⁶ Demonstrating the reliability of web content can be a challenge.

The Federal Court of Appeal admitted records from the Web Archive (“the Way-Back Machine”) to show the use of trade marks at particular periods.²⁶⁷ While showing use of a mark in practice was arguably not hearsay, the court noted different sites that might be considered more or less reliable. Thus ‘official’ government sites might be more readily admissible than user-generated content.²⁶⁸ However useful they might be as a starting point for research, Wikipedia²⁶⁹ entries may be hard to get into court to show their truth. A US appellate court decided in April 2009 that the ability of any person to amend a Wikipedia entry makes information on the site too unreliable to use as evidence.²⁷⁰

The *Evidence Act* of Ontario provides that public documents are admissible without proof of authenticity.²⁷¹ The phrasing of these provisions seems to imply that they must be printed rather than published online. Many government reports these days are published only online. How does one then prove their content, if one does not have access to a live witness from the relevant jurisdiction to testify either directly about the content or at least with personal knowledge about the web publication?

A final point about official publications: in several Canadian jurisdictions the online versions of the statutes and regulations are considered official. New Brunswick does this by simple declaration online.²⁷² Ontario requires that the official copy be in a prescribed format, the choice being those currently found on the e-Laws web site.²⁷³ Part V of PIPEDA revised the federal *Statute Revision Act*²⁷⁴ in 2000 to permit electronic publishing of statutes; these provisions came into force on June 1, 2009.

(e) Weight of the Evidence

266 Electronic records may be real evidence rather than hearsay in some cases, though. *R. v McCulloch*, [1992] B.C.J. No. 2282 (B.C.Prov. Ct.).

267 *ITV Technologies Inc. v. WIC Television Ltd.*, 2003 FC 1056. The decision was upheld on appeal without further discussion on this point.

268 *Ibid.* para 16-17. In the U.S., official publications are self-authenticating even online. *Equal Opportunity Commission v. E.I. DuPont de Nemours and Co.*, 2004 U.S. Dist. LEXIS 20748 (E.D.La.20748). For private information, compare *Teddy St Clair v Johnny's Oyster and Shrimp Inc.*, 76 F.Supp. 2D 773 (S.D.Tex. 1999), where the court refused to allow, as hearsay, “voodoo information taken from the Internet”.

269 Online: <http://en.wikipedia.org> .

270 *Palisades Collection v Graubard*, discussed in M.P.Gallagher, “Wikipedia too Malleable to be Reliable Evidence”, Law.com Legal Technology, April 22, 2009, online:

<http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202430073269>. The information tendered demonstrated that a large bank had taken over a small one in 2004 – not hard to prove from other sources, and not personal to either party.

271 Evidence Act (Ontario), above, note 240, notably ss. 25 and 26. Other jurisdictions have similar provisions.

272 New Brunswick Queen's Printer, Acts and Regulations, online: <http://www.gnb.ca/0062/acts/index-e.asp>, though the printed version prevails if it is inconsistent with the online version. See the Queen's Printer's disclaimer, online: <http://www.gnb.ca/0062/acts/disclaimer-e.asp>. The government's general web disclaimer (linked to from the statutes and regulations page) takes the contents even further from official: <http://www.gnb.ca/include/root/include/disclaimer-e.asp>

273 See online: <http://www.e-laws.gov.on.ca>, The *Legislation Act, 2006*, S.O. 2006 c. 19 Sched F., ss. 35, 38 and 39 make the prescribed form of an official copy of the law admissible, and O.Reg.413/08 prescribes the form. Note that the official status is subject to time limits as well, so one can search for official versions as they were at a given time.

274 The Act was renamed the *Legislation Revision and Consolidation Act*, still cited as R.S.C. 1985 c. S.20. See now s. 21 on electronic publishing and s. 31 on the evidentiary value of the print and electronic form of the laws..

Having found the evidence through the discovery process and satisfied the tests for its admissibility, counsel still must ensure that the court will find it persuasive. Generally statute law does not instruct the courts in how to weigh the probative value of evidence. The UN Model Law on Electronic Commerce says only that “[i]nformation in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regards shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.”²⁷⁵ This does not change Canadian law in any way, so it was not adopted in Canadian uniform legislation.

Two recent cases illustrate different limits to electronic evidence once admitted. In *Kerr v Dillard Stores*,²⁷⁶ an employer alleged that an employee had electronically signed an agreement to arbitrate employment disputes. The employee denied signing. The employer pointed to company policies about keeping passwords secure and a system of confirmation emails after the signing of contracts, a kind of system-integrity argument in support of the authenticity of the signature on the file. The employee had almost never been online in the company system, and on the day the contract was alleged to have been signed, a supervisor had logged in with her password to demonstrate to her another aspect of the system. On balance, the court was unable to find that it was more likely than not that the contract had been signed.

One concludes that having sufficient system integrity to get the electronic record admitted is not necessarily enough evidence to make it persuasive, even when the integrity of the system is the key issue.²⁷⁷

One may submit as well that questions of authenticity of electronic records should be dealt with more often at the weight stage than in determining admissibility. Otherwise one risks creating expensive barriers to justice about evidence that is not seriously in question. Only when it is in question would one need to bring out the heavy artillery on the electronic records. Perhaps the court’s ability to sanction fruitless inquiries by cost orders would be appropriately exercised for exaggerated concerns about the admissibility of electronic evidence.²⁷⁸

In *Leoppky v. Manson*,²⁷⁹ an exchange of emails was admitted to show an agreement about a land transfer, and it was held to satisfy the Statute of Frauds’ requirement that the agreement must be in writing and signed. Nevertheless the court refused summary judgment because one party claimed to have reserved consent pending consultation with her lawyer. The emails were essentially silent on this point. So even admitted and credible evidence may still yield to oral evidence of other considerations. This is clearly true of any particular piece of evidence in whatever medium. The case just illustrates

275 MLEC, above, note 24, article 9(2).

276 *Kerr v Dillard Store Services Inc.*, __F.Supp. 2d_ (D. Kan. Feb. 17, 2009), online: <http://hr.cch.com/cases/Kerr.pdf>

277 The court did not discuss admissibility at all in the case. There may be conclusions about computer security here too, notably the vulnerability of authentication by shared secret. See above, TAN 119. However, given the employee’s lack of familiarity with and almost total lack of use of the computer system, it is hard to see what computer security measures would have made the employer’s case stronger.

278 The new rules favouring proportionality in procedures will apply here as well as at the discovery stage. See above note 222.

279 Above, note 66. Although Alberta had adopted the uniform legislation on electronic transactions and evidence discussed in this paper, the court did not find it necessary to refer to any of it.

that electronic evidence is subject to the same operating principles as other kinds of evidence.

4. Electronic practice of law

How does one practice law in the age of information technology? The question could be the subject of a full article on its own. Here we will say only that it is dangerous to practise law without some knowledge of the characteristics and risks of electronic records and communications. It is arguable that practising without a solid knowledge of the implications of technology constitutes professional negligence.

One of the main questions in the area is how one communicates with clients. Lawyers often exchange emails with other lawyers and with their clients, commonly attaching confidential documents and discussing legal opinions, but seldom use encryption or other methods of ensuring the source, destination, integrity or confidentiality of the communications.²⁸⁰ The Law Society of Upper Canada's publication on this topic, "Ethical Considerations and Technology", admits that lawyers can treat the Internet with reasonable expectations of privacy. It is not a breach of the duty of confidentiality owed to one's clients to communicate without encryption.²⁸¹

However, lawyers are expected to be reasonably familiar with security issues online and to govern themselves accordingly when particularly sensitive communications are involved.²⁸² One should be sure that the client knows the risks (which means that the lawyer has to know them, in order to estimate the client's knowledge) and (ideally) expressly accepts them with an informed consent. The appropriate method of communications may vary with the sensitivity of the matters being communicated.²⁸³

Some particularly cautious lawyers hesitate to publicize their e-mail addresses for fear of being placed in an awkward position if potential clients e-mail them confidential information before they have had the opportunity to run a proper conflicts check. One sees emails with multiple disclaimers – usually at the end, so the reader does not see them until he or she has read the whole document, when it may be too late. One web page notice dealing with confidential information reads "Any unsolicited information sent to [the author] cannot be considered to be solicitor-client privileged."²⁸⁴ Others, more general, caution that the email or use of a web site does not in itself constitute a lawyer-client relationship. One memorable email note of this kind said "If this were legal advice, there would be an invoice attached."

280 Encryption used to authenticate source or integrity of a document does not necessarily fulfill its traditional function of maintaining confidentiality of the information.

281 Law Society of Upper Canada, "Ethical Considerations and Technology" (2001), based on a Federation of Law Societies document originating in Alberta, online at http://rc.lsuc.on.ca/pdf/pmg/tech_guidelines.pdf. See page 3. Compare American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Op. 99-413 (1999).

282 *Ibid.* and see Law PRO, *Managing the Security and Privacy of electronic data in a law office* (2005), online: <http://www.practicepro.ca/practice/pdf/ManagingSecurityPrivacy.pdf>

283 See the Law Society of Upper Canada, *Practice Management Guidelines: Technology*, s.5.7, 'confidentiality', online: <http://rc.lsuc.on.ca/jsp/pmg/technology.jsp#s57>.

284 David Fraser of McInnes Cooper, Halifax, in Canadian Privacy Law Blog, online: <http://www.privacylawyer.ca/blog/>.

The impact of law firms' web sites on the practice can be important too. Besides the normal restrictions on advertising, which are becoming more and more relaxed in any event, providing legal information on web sites raises issues of negligence if it is taken as advice, and of unauthorized practice if it is read in jurisdictions where the authors are not entitled to practice.²⁸⁵ Disclaiming the giving of legal advice, or of creating a lawyer-client relationship, while clearly advisable, raises questions whether such web site terms of use are enforceable, especially when the reader is not required expressly to acknowledge being bound by them.²⁸⁶

Four sources among many of good practical advice will be mentioned here.

- The Canadian Judicial Council has issued a “National Model Practice Direction For the Use of Technology in Civil Litigation.”²⁸⁷ It provides “a Court approved framework for managing both Hard Copy and electronic Documents in a Technology environment.”
- The Canadian Bar Association has published “Guidelines for Practising Ethically with New Information Technologies”, a supplement to its code of professional conduct.²⁸⁸ A popular compilation of articles about the “virtual law firm” appears in the CBA's magazine *The National*.²⁸⁹
- LawPRO, the Ontario lawyers' professional insurance company, publishes many guidelines to lawyers on how to avoid malpractice claims. It has been active through this PracticePRO site to advise on technology issues.²⁹⁰ Notable articles among many include “Why electronic documents are different”, “Technology: Good Tool, Bad Tool”, and “If you do nothing else – the lucky 13 things you must do to protect your data.” The information is accessible and focused.
- The American Bar Association has run for several years an annual conference known as LawTech²⁹¹ that offers practical advice and demonstrations by vendors and neutral commentators. Canadians seem to benefit from attending.

VII. EMERGING ISSUES

This final section sketches a few important developments that will affect the practice or substance of law in the foreseeable future. In information technology, the foreseeable future is not a long time.

1. Web 2.0

285 S. Kimbro, “Avoiding the Unauthorized Practice of Law (UPL) in other Jurisdictions with a virtual law office” (Part one), December 2008, online: <http://virtuallawpractice.org/2008/12/08/avoiding-the-unauthorized-practice-of-law-upl-in-other-jurisdictions-with-a-virtual-law-office-part-one/>.

286 The enforceability of “browsewrap” terms, i.e. those asserted to apply to someone browsing on the web, as distinct from “clickwrap” or “click-through” contracts, is open to debate. See the discussion above, TAN 84.

287 The direction (2008) is online: [http://www.cjc-ccm.gc.ca/cmslib/general/JTAC%20National%20Model%20Practic\(1\).pdf](http://www.cjc-ccm.gc.ca/cmslib/general/JTAC%20National%20Model%20Practic(1).pdf).

288 The Guidelines were published in 2008 and are online: <http://www.cba.org/CBA/activities/pdf/guidelines-eng.pdf>. Comments by X. Beauchamp-Tremblay on how to implement them in practice are found in the Slaw blog, online: <http://www.slaw.ca/2008/12/06/meat-on-the-bone%20A0-comments-on-the-guidelines-for-practicing-ethically-with-new-information-technologies>.

289 The (CBA) National Magazine Online Supplement, June 2009, online: <http://www.cba.org/cba/PracticeLink/national/virtuallaw.aspx>.

290 See the PracticePRO technology site, online: <http://www.practicepro.ca/technology/default.asp>. The American Bar Association also has a compendium site on the topic, online: http://www.americanbar.org/groups/departments_offices/legal_technology_resources.html.

291 See online: <http://apps.americanbar.org/techshow/>.

The term “Web 2.0” designates a number of more or less related technological developments that tend to feature interactivity between users and web sites, not just for simple commercial transactions, but where users influence the content of the web sites and have data stored or processed online. Far more information is deliberately shared with web servers than in traditional uses, where the Internet was more of a method of point-to-point communication than a method of managing data.²⁹² A current catchphrase for business applications of this kind of world is “cloud computing”,²⁹³ where the data are out “in the cloud” rather than located on the owner’s server.

This set of phenomena raises difficult questions of authentication, both to the server and to the user, and of integrity of the data going either way. Liability issues are multiplied with this kind of web service too, since it can be unclear who is responsible for the sites or just what they are promising to do and for how long (what happens when they discontinue the service?), not to mention the perennial question of the effect of disclaimers.

Evidentiary issues also arise in cloud computing, and indeed in many web-based applications. It is harder to meet the criteria discussed in the e-evidence sections above. Such applications often use non-standard (not 90+% Microsoft, like office documents) and proprietary software whose reliability is hard to evaluate, much less prove. The consumer focused applications like social networks may be intentionally less rigorous about security, for ease of use. One may have to look to the Internet service providers and Internet Protocol information to support authentication, rather than information closer to the record system itself. It may be hard to persuade a court that web service providers should be considered third parties whose systems can be presumed to be reliable, under the Uniform Electronic Evidence Act.²⁹⁴

Web 2.0 relations often involve the transmission of personal information to the web sites in ways that allow for ready re-use. For example, social networking sites like Facebook or MySpace (and a vast number of others, including many directed at children) and search engines like Google routinely collect information from browsing habits and from comments posted on the site and target advertising at the users based on this information. That may suit the users’ purposes or make them uncomfortable, depending on the person.²⁹⁵ The Federal Trade Commission has reviewed this phenomenon too and has cautioned users and merchants about its privacy risks.²⁹⁶ And the operators of the sites themselves have legal issues about how to protect themselves from what the users may do.²⁹⁷

292 A dramatic American list of issues appears in R. Needleman, “Legal Suicide for Web 2.0 Startups: A beginner’s guide”, Webware September 20, 2007, online: http://news.cnet.com/8301-17939_109-9782365-2.html.

293 A useful outline appears in the Wikipedia article, online: http://en.wikipedia.org/wiki/Cloud_computing. The government of the United Kingdom declared in June 2009 that all governmental IT purchases should be made with a view to being compatible with cloud computing. Out-law.com, “UK Government commits to cloud computing for public sector”, June 23, 2009, online: <http://www.out-law.com/page-10114>.

294 See above, note 257.

295 For a recent example of claims to and uses of personal information, see S. Fodden, “Your License on Facebook” on the Slaw blog, February 8, 2009, online at <http://www.slaw.ca/2009/02/08/your-license-on-facebook/> Note Connie Crosby’s anecdote in the third comment.

296 Federal Trade Commission, Staff Report, “Self-Regulatory Principles for Online Behavioral Advertising”, February 2009, online: <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>. One Commissioner’s concern about the readiness for self-regulation is online: <http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf>.

297 P. Viscounty et al, “Social Networking and the Law: Virtual Social Communities are Creating Real Legal Issues”, (2009), 18 *Business Law Today*, No. 4, March-April 2009, online: <http://apps.americanbar.org/buslaw/blt/2009-03->

Another element of the power of users is their ability to organize information as they see fit, through tagging. People apply their own subject labels to materials found online, from pictures to videos to documents to web sites, so that they can find them again later. This gives the individual user great power to organize random information in a way most useful to that individual. It may be a promising way to start, if not finish, legal research. (One sees as well the use of search tools designed for the Internet, such as Google, to organize and locate items in one's own electronic records.)

Tags can be shared, and web sites can aggregate the tags, so that others' labels are accessible to everyone, with links to the material to which they have attached the label. Thus the meaning of the labels or tags is ultimately determined by the users as an unrelated but interested group. This leads to "folksonomies", a play on the word "taxonomy", but with the classification inherent in that term being performed by "folk culture". This leads to different ways of accessing information online, and arguably different ways of thinking about the information. Perhaps it leads to the Wisdom of Crowds.²⁹⁸

2. User-generated content

As a possible subset of Web 2.0 issues, but big enough to mention on its own, one finds questions relating to online publications posted by individuals or businesses other than mainstream publishers. This "user-generated content" is often produced without legal advice or even any idea that legal issues may arise. A few examples of user-generated content give the idea of the scope of possible issues:

- Wikis that allow readers to contribute material and edit it. The prime example is Wikipedia,²⁹⁹ a user-generated encyclopedia available in many languages. Legal wikis exist as well, including Jurispedia³⁰⁰, a multinational effort, and many others.³⁰¹ They may be more or less tools of collaboration among known contributors, or open to the world.
- Fan fiction: readers invent and publish stories based on books, television or movies, using characters and characteristics of those copyrighted works.
- Blogs involving comment on current issues, people or even the law.³⁰²
- Social networking sites like Facebook³⁰³ and MySpace³⁰⁴ as well as more specialized sites for photographs³⁰⁵ and almost any other focus imaginable.
- At time of writing the most recent phenomenon, Twitter³⁰⁶ appears to be part social medium, part

[04/viscounty.shtml](#).

298 J. Surowieki, *The Wisdom of Crowds*, (Random House: 2004), online:

<http://www.randomhouse.com/features/wisdomofcrowds/>.

299 Online: <http://www.wikipedia.org>. Its use as evidence was mentioned above TAN 262.

300 Online: <http://www.jurispedia.org/>

301 See R. Ambrogi, "Legal Wikis are Bound to Wow You", Law Technology News, May 7, 2007, online:

<http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1178541412778>. Some lawyers are using wikis as collaborative drafting tools with colleagues or clients within secure networks.

302 Anne Helmond, "How Many Blogs are there? Is someone still counting?", The Blog Herald, February 11, 2008, online: <http://www.blogherald.com/2008/02/11/how-many-blogs-are-there-is-someone-still-counting/>. Canadian blogs about law are listed online: <http://www.lawblogs.ca/>.

303 Online: <http://www.facebook.com>

304 Online: <http://www.myspace.com>

305 For example Flickr, now owned by Yahoo!, online: <http://www.flickr.com>, though Facebook and such sites often contain photos too.

306 Online: <http://www.twitter.com>

blog. Its uses in general are expanding rapidly, and lawyers are finding ways to build professional advantages from it.³⁰⁷

Legal issues run a wide range here. A list by the Electronic Frontier Foundation as part of its “boot camp” on such matters³⁰⁸ included:

- Defamation, harassment, and other accusations of bad behavior.
- Breaches of privacy – one's own, exposing oneself to risk, or that of other people.³⁰⁹
- Intellectual property generally: fair use, free culture, and the right to remix, take-downs and put-backs, uploading and downloading content, and Creative Commons licences (“some rights reserved”³¹⁰).
- How to respond to cops, crooks, and courts who want your customers' communications and other private information.³¹¹
- The rights of anonymous speakers³¹².
- Porn, predators, and the pressure to police those who may use web sites that one puts up for one's own content.
- Webcasting and what to do when you've been hacked.

One might add that the questions of liability of intermediaries, notably ISPs, for user-generated content are as intense here as for professionally-created content, and the liability for passing on security threats is also relevant.³¹³

Canadian legal authorities have focused mainly on the intellectual property issues to date.³¹⁴ Some attention has also been paid to the employment consequences of online self-expression, such as through blogs. Employers should have clear policies about what is acceptable conduct and take care that the policies are known by employees. Employers may be concerned not only about their reputation as expressed by their employees but also breaches of confidentiality with practical or even legal consequences, such as revealing material changes without the formalities of filings under securities law³¹⁵ or losing claims to a trade secret because of an employee's disclosure of it.³¹⁶

307 See for example S. Matthews, “Lawyer' Twitter Practices: 29 Do's and Don'ts”, April 25, 2009, online:<http://www.slaw.ca/2009/04/25/lawyer-twitter-practices-29-do%e2%80%99s-and-don%e2%80%99ts/>.

308 EFF Bootcamp 2009, online: <https://www.eff.org/bootcamp/>

309 The disclosure of personal information on such sites is discussed above, TAN 232.

310 See the Creative Commons licence online: <http://creativecommons.org>, and its Canadian version online: <http://wiki.creativecommons.org/Canada>.

311 Above, note 235.

312 The ability of the courts to compel disclosure of identity or identifying information was discussed above, TAN 231. On the principles of anonymity and identity issues, see the University of Ottawa's project “On the Identity Trail”, online: <http://www.idtrail.org/>.

313 See discussion above TAN 180.

314 See for example G. Westcott, “Friction over Fan Fiction”, *Literary Review of Canada*, July 2008, online: <http://reviewcanada.ca/essays/2008/07/01/friction-over-fan-fiction/>; and R. Shoyama, “Intelligent Agents: Authors, Makers and Owners of Computer-generated Works in Canadian Copyright Law”, (2005), 4 *Cdn Journal of Law and Technology* No. 2 p. 129, online: http://cjlt.dal.ca/vol4_no2/pdfarticles/shoyama.pdf.

315 One financial analyst who promoted his blog with Twitter feeds had to develop a four-part (“four tweet”) disclaimer to satisfy securities regulations. McDermott Will & Emery, *Informal Corporate Disclosure in the Age of Twitter*, May 20, 2009, online: <http://www.mwe.com/info/news/wp0509b.pdf> at page 3 footnote 3 (and for presentations and related materials on this topic: <http://www.mwe.com/info/twitter0509/>).

316 Such policies should be tailored to the employer's culture, while recognizing the inevitability of employees' use of

3. Virtual worlds

Another electronic field rich in possibilities is virtual reality. This phrase refers to online environments (created by real service providers) that feel like a “world” of experience. Some multi-player role-playing games are like this: World of Warcraft is often mentioned as an example.³¹⁷ Whole “world” sites, where players participate through an imaged representative usually called an “avatar”, include Second Life³¹⁸ and many others. Where a game stops and a world stops is not a matter for unanimity. Second Life allows its members to buy and sell property (including converting the currency of the virtual world to U.S. dollars)³¹⁹ and to enter into many kinds of relationships. For a time Second Life featured a real-time casino, in which real money could be made or lost; the casino was shut down due to legal pressure from real-world authorities.³²⁰ Businesses have opened stores in Second Life that allow sales with online currency, and countries have had embassies on it. Law firms are there too;³²¹ at least one Canadian law firm had a virtual law office there.³²²

Life in virtual worlds encounters a range of legal issues. Does one have a property interest in one’s virtual assets? Different service providers have different rules on one’s right to buy and sell “in-world” assets for real money, but online auction sites exist where they are traded in any event. How enforceable are the terms of service? Is the whole “world” a creature of a contract of adhesion? Is in-world income taxable in the real world? To what extent can the service providers assert ownership over any intellectual creations devised by participants in the virtual world? Can one’s membership be revoked without cause?³²³ The scope of influence between the virtual and the real world is still

social media as well as both sides' legal rights and duties. Two well-regarded American examples are the policies of Sun Microsystems, “Sun Guidelines on Public Discourse”, online: https://www.privacyassociation.org/assets/presentations/09Academy/Employer_Policies_H2.pdf; and those of Intel, “Intel Social Media Guidelines”, online: <http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html>

317 The World of Warcraft site is online: <http://us.battle.net/wow/en/>. The legal documents are at: http://us.blizzard.com/en-us/company/legal/wow_tou.html.

318 The Second Life site is online: <http://secondlife.com/> Its terms of service are at: <http://secondlife.com/corporate/tos.php>

319 The Second Life marketplace is described online: <http://secondlife.com/whatis/marketplace.php>.

320 Linden Laboratories explained its policy on its Second Life blog, online:

<http://community.secondlife.com/t5/Features/Wagering-In-Second-Life-New-Policy/ba-p/585072>. However, the urge to gamble has been one of the main sources of innovation on the Internet. An overview of the issues and sometimes excuses is online: <http://medialoper.com/second-life-vice-linden-lab-is-in-denial-about-its-gambling-problem/>

321 L. Benetton, “Lawyers hang their virtual shingles online in Second Life”, Lawyers Weekly September 7, 2007, online: <http://www.lawyersweekly.ca/index.php?section=article&articleid=535>. At least one firm derives about a quarter of its revenue from such work: C. Kirby, “Avatars, attorneys in new world of virtual law”, San Francisco Chronicle, April 27, 2009, online: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/26/BUH0172A42.DTL>.

322 Davis LLP was represented in Second Life. No legal advice is given directly, but it provided a method to meet potential clients and discuss issues in a general way. However, the firm has now closed that office. M. Kowalski, “Davis LLP closes virtual office”, FP Legal Post, January 12, 2009, online: <http://bit.ly/qZmHNNH>. The firm maintains its Video-Game Law Blog, online: http://www.davis.ca/community/blogs/video_games/

323 K. Craig, “Second Life Land Deal Goes Sour”, Wired, May 18, 2006, online:

<http://www.wired.com/gaming/virtualworlds/news/2006/05/70909>. The member won a decision that the membership agreement was not binding: *Bragg v Linden Research Inc.*, 487 F.Supp. 2d 513 (ED Pa. 2007). The case was settled before judgment, allowing the member back on Second Life. Technical arguments are described in detail on B. Duranske, Virtually Blind blog, online: <http://virtuallyblind.com/2007/10/04/bragg-linden-lab-settlement/>.

developing.³²⁴ These issues have been analysed by articles in Canada,³²⁵ by a recent book in the US,³²⁶ and by a working group of a European Union network security group,³²⁷ but the last word is not yet spoken.

VII. CONCLUSION

That comment can serve as the conclusion to this article as a whole. One does not expect the “last word” on the legal impact of electronic communications in the near future. Technological changes drive legal changes, and the technology is in constant rapid evolution.

For a while there was a debate whether electronic communications made up a different kind of law. A negative view said that electronics merely provided a medium, and just as there was no “law of the horse” in the nineteenth century, though many aspects of life depended on horses, so too the law of electronic communications was not a separate discipline.³²⁸ A noted response to this argument underlined a number of ways in which legal relationships operated in cyberspace that had a real impact on how law regulated conduct, and these operations were worthy of study for the light they cast on legal regulation in general.³²⁹

The distinction begins with the architecture of cyberspace – the programs, protocols and even hardware that determine what one can see, what one cannot see, and which messages are transmitted in what manner. Choices about architecture may make activities with legal or social consequences easier or harder than they would be offline. Preventing access to “adult” goods by minors is harder. Tracking people's choices is easier. Yet rules of law can affect the architecture, which in turn affects our ability to regulate activities we decide need regulation. This dynamic teaches us useful lessons about the variety of tools available to promote society's values in “real world” relationships.³³⁰

Recently a colloquium at the Université de Montréal re-examined the question “Is E-Commerce Law Different?” by way of noting the passage of fifteen years since the invention of the World Wide Web and the effective opening of the Internet to commercial uses.³³¹ The answer is less important than the

324 A woman obtained a divorce in England against her husband because of his virtual relationship with another woman. S. de Bruxelles, “Second Life affair leads to real-life divorce for David Pollard, aka Dave Barny”, Times Online, November 20, 2008, online: http://women.timesonline.co.uk/tol/life_and_style/women/relationships/article5151126.ece. A woman in Japan was prosecuted for “killing” her husband’s avatar. K. Parrish, “Japanese Woman Kills Online Husband”, Tom's Guide, October 27, 2008, online: <http://www.tomsguide.com/us/Maple-Story-Virtual-Divorce.news-2838.html>. In China, someone killed another player of an online game because the victim had stolen or destroyed his online property. Reuters, “Gamer gets life for murder over virtual sword”, June 9, 2005, online: <http://news.bbc.co.uk/2/hi/technology/4072704.stm>.

325 S. Abramovitch and D. Cummings, “Virtual Property, Real Law: The Regulation of Property in Video Games”, (2007), 6 Cdn Journal of Law and Technology No. 2, p. 73; D. Spratley, “Virtual Property and the Law”, Davis & Company LLP, Spring 2006, online: <http://www.davis.ca/publication/Virtual-Property-and-the-Law.pdf>.

326 B. Duranske, *Virtual Law: Navigating the Legal Landscape of Virtual Worlds* (American Bar Association: 2008).

327 European Network and Information Security Agency (ENISA), *Virtual Worlds, Real Money*, (2008), online: <http://bit.ly/oA3Ova>.

328 F. Easterbrook, “Cyberspace and the Law of the Horse” 1996 U. Chicago Legal Forum 207

329 L. Lessig, “The Law of the Horse: What Cyberlaw Might Teach”, (1999) 113 Harvard L.R. 501, online: <http://www.lessig.org/content/articles/works/finalhls.pdf>.

330 *Ibid.*

331 “Is E-Commerce Different?”, proceedings of a colloquium in Montreal, October 2008, online:

discussion of the question. There is no doubt that most areas of the law are touched, as are most areas of human activity, by electronics, and the law in almost all fields now incorporates responses to the use of technology.

Law reform, through the courts and the legislatures, and private arrangements through contract and technological measures, have framed these responses. Whether they are the right framework and whether more or different rules are needed is an ongoing discussion. Meanwhile, practitioners work to understand the challenges and use the laws to promote their clients' interests, and contribute in doing so to the evolution in their turn.

[June 2009]