Canadian Journal of Law and Technology

Volume 1 | Number 2 Article 1

4-1-2002

Solving Legal Issues in Electronic Government: Authority and Authentication

John D. Gregory

Solving Legal Issues in Electronic Government: Authority and Authentication

John D. Gregory†

Introduction

This article is an overview of some of the legal themes and issues faced by governments in the electronic age, with particular regard to their own operations: electronic service delivery and the administration of government itself.

Electronic government is the performance of any function of government using electronic records and electronic communications. It may involve, in the language of the *Uniform Electronic Commerce Act*, "us[ing] electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with documents or information."[1] The term thus covers the provision of governmental services to the public, including communication from the public to the government. It also extends to the "back office" of government, the methods of public administration within the Executive Branch of government and between government and those who supply goods and services to it.

The term is sometimes used to extend to regulation of private activities carried on electronically, either as extensions of traditional activity or as new types of conduct made available by means of electronic communications. The current paper does not address such questions.

Is electronic government legal?

For the private sector, individuals or businesses may ask their lawyers in respect of a proposed activity, "is it legal?", often meaning not "is it permitted?" but rather "is it effective?". Will they have enforceable rights in law if they engage in a particular activity by electronic means?

For government, the question "is it legal?" is also one of legitimacy: is it right for the government to act in this way? Legitimacy may express itself through expressions of authority to act, which is related to but not the same as saying that an action is not illegal. In some settings, the legitimacy of government action will affect the enforceability of the action, either on the part of government against a person subject to that government's rule, or on the part of a private citizen against the government.

In general, the senior levels of government in Canada — the federal and provincial governments — have the authority they need to carry on their operations electronically. The Crown, in right of Canada or the provinces, has the powers of a natural person,[2] who can choose how to communicate. These powers are subject to the usual constitutional and sometimes statutory limits, and the limits need to be addressed in some cases to ensure appropriate electronic conduct. Public bodies that have only powers conferred by statute have needed more legislative help in acting electronically, as we will see later.

Legitimacy can also turn on other standards of appropriateness. Here we will look briefly at some of the qualities electronic government action should have, or some of the standards it should meet, in order to achieve the desired level of legitimacy. Is it acceptable for a government to act in this way? Is the use of electronic records effective as an act of government? A later section will examine in more detail law reform in support of electronic government.

Much of what a government, or those who deal with a government, look for in its electronic communications is common to public and private sectors. For example, any user of electronic communications wants a degree of assurance as to the security of the communications and their source: who sent them? Any user is interested in the integrity of the information communicated, in the sense that it is trustworthy, and that it has not been altered since it was sent. Any user wants an efficient system.

Similarly, both public and private sector users have an interest in the legal regime to which their electronic communications are subjected. Whose law applies to them, what courts or other bodies get to dispose of them, and how can any judgments be enforced in places other than where they were made?

---

†General Counsel, Policy Branch, Ministry of the Attorney General, Ontario. This paper was developed from a presentation sponsored by the Centre for Innovation Law and Policy at the Faculty of Law, University of Toronto. The views expressed are not necessarily those of the Ministry or of the Faculty. Thanks to Troy Harrison, Charlotte Judd, Rhonda Lazarus, Jinyan Li, Michael Power, Jeanne Proulx and Karen Wold for their helpful comments on versions of this paper, and to Mark Ratner and Kajal Khanna for tracking down some necessary notes.

Some elements of legitimate governmental communications are, however, unique to the public sector. For example, governments in Canada are subject to detailed rules about the privacy of personal information in a way that is novel and less extensive for private sector bodies.[3] Electronic communications seem particularly susceptible to attacks on privacy, so government is called upon to be cautious in this domain.

Likewise, the fairness of public use of electronic communications is a more pressing value than it is for private actors. Fair access to public services is one element of this question, and an element of a duty to work against a "digital divide" that may prejudice citizens and businesses less able than others to profit from electronics.[4] At some point, the guarantee of equality under the law could impose constitutional limits on governments' ability to move wholly online.

Governments have both a constitutional and a statutory duty to be open to citizens and to provide access to information.[5] They also have what one might call a duty to history, i.e., to maintain official records in a permanently accessible way.[6] Transitory communications have to take this into account, and storing electronic records over time is a special challenge because of the impermanence of storage media and the evolution of hardware and software used to create and read electronic information.[7]

Government documents are often official, since they carry special weight of authority or special legal effect from their status. One sees this in the priority they are frequently given in evidence statutes.[8] This may be considered a higher form of authenticity accorded to these records, but it has an impact on the demands made of electronic communications so that they will deserve the same respect that paper documents receive. Pushing this theme further, it can be argued that the integrity that the public expects of government communications is not just that they be unaltered but that their content be true. That is not a question of the medium used.

Finally, government use of electronic communications has to be politically acceptable to the opinion-makers of a society. No amount of technical excellence can guarantee that any manifestation of electronic government will meet this standard. One does hear from politicians, and sometimes from business people, that government should lead the way to making people confident about electronic communications being safe and effective. Government should be a "model user" of the technologies.[9] This is a technical aspect of the legitimacy argument, that proper government use can buttress and encourage general use of paperless records. It overlaps, not always comfortably, with another function of government, business promotion, and particularly, the promotion of e-business.

Not all these qualities, or their absence, have direct legal consequences. Different government programs will have different priorities among them, and some factors will play more important roles in some governments or disciplines than in others. Nevertheless, anyone wishing to evaluate the legality — in the broad sense — of electronic government would do well to keep these criteria in mind and measure the methods of communications and the authority and practice of electronic government initiatives against them.

How legitimacy and legality have been achieved or may be achieved is the subject of the rest of this article. We will look at a number of Ontario government initiatives, with glances beyond the provincial borders, to give an impression of the range of and the legal authority for electronic programs, popularly known as electronic service delivery (ESD). The principal part of the discussion deals with authentication, both of information coming into government and of that going out from government, and looks at some of the legal options available. Next, we consider the different issues involved in electronic administration — the use of electronic media within government or with its business partners. When we look at government's use of electronic communications for its own purposes, external or internal, we find a few of the qualities mentioned above predominate. Sometimes their importance is expressed, and sometimes it is simply a condition of doing business electronically that controls the options available. We finish with a review of law reforms that have supported more extensive use of ESD and e-administration.[10]

Electronic Service Delivery

Examples of electronic service delivery

The earliest service delivered electronically to the public by governments, as by the private sector, was information. The Internet is a marvellous method of distributing information widely and cheaply. Many government (and private) Web sites to this day provide only information. Sometimes, they extend this to include forms, such as applications for jobs or licences, that can be downloaded, printed, and filled in like any other paper form. The usefulness of these functions is great. The legal issues they raise are those of providing information in any medium: what happens if the information is wrong, incomplete or out of date? Although the public may expect Internet information to be more current than documents on paper, the usual array of legal tools — cautions, disclaimers, and the like — should suffice to keep liability within reasonable limits.[11] As a result, this article will not discuss them further.

When it moves beyond passive provision of information, electronic service delivery is the public sector equivalent of Business to Consumer (B2C) electronic commerce. It focuses on transactions between government and individuals, and individual businesses. A great deal of effort is being devoted across the country[12] and

elsewhere[13] to seizing the opportunities that ESD is thought to offer, in everything from issuing hunting licences to providing telehealth services to collecting fines — even to running electronic courthouses.

The government has been dealing electronically with the public in some areas for many years. For example, registrations of financing statements under the *Personal Property Security Act*[14] have been submitted in electronic form since the early 1990s. Land registration using electronic documents is spreading across the province since it began in 1999.[15] The Family Responsibility Office collects support payments from debtors and debtors' employers electronically and remits payments electronically to those entitled to them.[16] The Ontario Energy Board has established an electronic regulatory project, in collaboration with the National Energy Board and the energy industry, to allow applicants and intervenors to prepare electronic files and communicate across the country by electronic means.[17]

The trend in recent years has been towards more comprehensive programs, supported by broad enabling legislation. Ontario has been offering a "one-window" approach to business registrations through "Ontario Business Connects".[18] This permits access not only to provincial services such as getting a retail sales tax permit and an employer health tax licence, but also provides links to federal government sites to permit registration for business numbers for the Goods and Services Tax. The programs behind the electronic façade have also been adjusted to make their electronic delivery more efficient. Thus, Ontario is creating a "Master Business Licence" to replace a number of individual licences for different aspects of a business's operations.[19] This is only one example of a general rethinking of operational practices required by going electronic, rather than simply putting existing communications models online. It sometimes involves rethinking the broader statutory framework as well.

For dealings between government and individuals, the Ontario government is also offering a one-window service under the generic heading "Online Services"[20] (formerly known as Service Ontario). The home page offers special access to transactions involving school and work, driving, outdoors and recreation, health and social services, and "life events" (now limited to getting married and losing your wallet). This kind of service is becoming well established elsewhere. In Canada, New Brunswick has been a pioneer with Service New Brunswick.[21] One of the most extensive programs is in Singapore, with its eCitizen site,[22] which offers headings on Business, Employment, Housing, Defence (compulsory military service details), Family, Law and Order (file a police report, declare bankruptcy, etc.), Education, Health and Transport.

Comprehensive sectoral initiatives are also under way in Ontario and elsewhere. For example, the Integrated Justice Project[23] aims to harmonize data management practices throughout the justice system, across several ministries, and let the public deal electronically with the courts. Land information is collected, managed and made accessible to users through Land Information Ontario,[24] to provide a harmonized approach to information about property boundaries, and boundaries of cities and towns; zoning, land-use, assessments and mining rights information; population information (e.g., demographics and census data); topographic features (e.g., elevation, contours, streams, etc.); information about water, soils, plants, trees, fish and wildlife; water and air quality information; roads and civic addressing data and structures built on the land, such as utilities and buildings.

Authentication

Authentication is an element of security. We will situate it very briefly in this wider context, then look at some questions of principle touching authentication, and finally review how it has been sought in practice.

Security can be divided into two elements: network security and document security. The network — mainly for purposes of this paper, the Internet, but closed systems like linked public workstations or kiosks and internal government networks are also relevant — must be kept in operation, not subject to overloads or attacks or harmful interference, voluntary or involuntary, mechanical or human.[25] Security is never absolute; it is relative. Communications channels are more or less secure. The legal implication of an insecure network is caution about what one commits to the network, and how one keeps backup copies of documents.

The second element of security is document security, which essentially influences how sure one can be of the answers to three questions: what, who and where. Document integrity is the first: has the document been altered from what was intended by the parties to a communication? The practical issue for integrity is how one keeps one's data from being altered inappropriately or from being accessed or destroyed by unauthorized persons. Document source is the second element: who made the document and who sent it? This is usually known as the question of authentication.[26] The issue for authentication is how one can be sufficiently sure that one knows who one is dealing with.[27] Document origin is the third element: from what place did it come, and what legal regime applies to it? The issue of place is not dealt with in this paper. It is often discussed under the title of "jurisdiction".[28] Document security too is a question of degree: what level of assurance does one need in order to trust a document, or to give it legal consequences?

Some documents must also meet another criterion of security: is it confidential, i.e., accessible only to authorized readers or users?

The challenges for government here are not radically different from those faced by the private sector,

with two possible exceptions. First, government may be less tolerant of risk, for a combination of political and institutional factors. If you have a statutory duty to provide a service or pay money, and that service or money may make a very big difference to the lives of the people entitled to it, then you want to be sure that you are providing the service or paying the money to the right person. Moreover, the desire to be even-handed and accountable for compliance with rules, regulations and forms can lead to an over-diligent reliance on tried and true methods, known in extreme cases as "red tape". Add to this the professional reserve of lawyers, and one ends up being cautious and perhaps embracing technology only gingerly.

The second difference in security analysis within government is the large scale on which many programs are to operate. Ontario has twelve million residents entitled to health cards. Protecting the data from interception, and setting up a reliable identification and verification system for that many people, in a system that should not deny anyone vital services, is a different order of task from communicating with modest numbers of business customers.

It is worth looking more closely at authentication. The term "authentication" itself does not have a very clear meaning in Canadian law, outside perhaps the law of evidence. In the law of evidence, to authenticate a document means to provide evidence that can support a finding that the document is what it purports to be.[29] General usage of the term deals largely with source, and sometimes with the integrity of the document, i.e., whether it has been altered. My own view is that authentication is best restricted to verifying the source of a document rather than its integrity.[30]

How does the government know who it is dealing with? To a lesser extent, how do people dealing with the government know that they are really dealing with the government? There are two elements to this function: identification — determining who a person is in the first place; and verification — determining that a person claiming to be the identified person really is that person.[31]

There is a tension between authentication (identifying people and verifying their identity) and privacy (preserving personal information from undue disclosure). Governments have records that can be used to identify people reliably, but privacy laws[32] limit such activity to known programs and information collected in anticipation of those programs. Privacy statutes, such as Ontario's, make it difficult to pass information from one part of the government to another, because of the importance to the Act of "institutions", which are individual ministries or agencies. These rules reduce the benefit of some of the main features of electronic databases, which is their ability to search and compare records. All government electronic service programs have to accommodate the demands of the privacy legislation.[33]

In practice, much of the discussion of authentication turns on the use of signatures, and for new media, on the characteristics of electronic signatures. Ink-on-paper signatures are of very little use in demonstrating the integrity of a signed document, especially the pages of the document that are not signed.[34] That being said, the analysis of the appropriateness of different methods of verifying the source of a document can often influence the choice of method for verifying integrity. Likewise, the methods used for higher levels of assurance of source may also contribute to assurance of integrity.

The discussion can be made more concrete by looking at the ways that government in Ontario has dealt with requirements for signatures in different programs that have acquired an electronic version. The difference in treatment results from a formal process called "threat-risk analysis" (TRA). This involves evaluating how vulnerable a communications system is to compromise; how likely such compromise is (depending upon the incentives, financial or other, for people to try to compromise it); how serious the loss from a compromise is; how costly it is to secure the system against compromise, and what benefit flows from communicating electronically rather than sticking to paper; and how secure the paper communications are in the first place. Not all the programs mentioned here have been subjected to a full TRA, but the reasoning no doubt ran along these lines in any event.[35]

In general, the common law does not require that a signature be in any particular form, so long as the attribution and intention to sign are clear.[36] So long as signatures were on paper, the formal requirements tended to go without saying. There is little caselaw, and what there is deals with signing authority or — especially in the United States — whether a particular method meets the Statute of Frauds rule that some documents needed to be signed to be enforceable.[37] Essentially, a signature is evidence of a person's connection with a document, and of the intention of that person with respect to the document.[38] This suggests that such evidence in electronic form could be satisfactory at common law, without statutory support. Nevertheless, most e-government initiatives have looked to formal authority to support their solutions to the signature or authentication problems they have faced.

Authenticating information coming into government

The first set of solutions deals with information coming into government that traditionally had been signed by the person submitting it. Ontario has used at least five methods to accept such information electronically.

Eliminate the signature requirement

The most dramatic method is to eliminate the need for a signature entirely. This has been done for filings of

business names and styles, for personal property security registration, and for land transfer registrations, with different programs to back them up. The *Business Regulation Reform Act, 1994*,[39] authorizes the Minister of Consumer and Commercial Relations (now called the Minister of Consumer and Business Services) to make regulations on the electronic form of any business information being submitted to the government of Ontario under any statute. The approval of the Minister responsible for the statute is needed for any regulation not under an MCCR (MCBS) Act. Under section 10, the Minister may, by regulation, dispense with signatures otherwise required, or provide for the methods to be used to sign electronically.

To date, the powers under this Act have been used for the filing of business name registrations and partnership registrations. The 1995 regulation[40] reads:

> 3. (2) A business that files a unified form in an electronic format under subsection (1) is not required to sign the form by electronic signature or by signature copied or reproduced in any other manner.

These forms are filed to give public notice of names by which corporations are doing business, so the public knows who the legal person is behind a business name. The paper forms were signed, but it was unlikely that anyone ever verified the signatures. No public benefits or grants were given for filing the forms. In short, there was little incentive for anyone to submit falsified forms, and little downside to the government if falsified forms were filed. The cost of verifying paper signatures, or of setting up a system of reliable electronic signatures, outweighed the cost of having compromised records enter the system.[41]

Electronic registration of financing statements under the *Personal Property Security Act*[42] was authorized by the *Electronic Registration Act (Ministry of Consumer and Commercial Relations Statutes) 1991*.[43] While signatures were not required on financing statements, those filing them were known to the Ministry, and they had to keep an account with the Ministry to pay for documents filed. The Ministry knew who it was dealing with and ran no risk of non-payment. The filings gave notice of security interests but did not constitute the security interest itself. As a result, wrongful filings could cause some loss to third parties, but not to the principal parties to the agreements.

Electronic registration of land transfers was authorized by 1994 amendments to the *Land Registration Reform Act*.[44] Agreements to transfer land no longer need to be signed, since they are no longer registered.[45] However, the registration of those documents occurs only on the strength of a request from a lawyer or other authorized party, who communicates with the land registry using a very secure digital signature.[46] Since the registry is the official record of the title, and much value is carried by title to land, security systems are vitally important, and the threat–risk analysis produces a different result than for business name registrations.

Close the system

The second technique, where one does not eliminate the signature requirement, is to close the communications system. A system is closed by technology, so one can identify all the potential signers by other means, or by contract, so one can bind them by contract to take responsibility for messages that appear to come from them. Generally, both techniques are used: the contract designates the technology to be used, so that its reliability will be satisfactory to the government. This closed system is widely used in the private sector; any electronic banking system depends on the contract between the customer and the bank. Likewise for government, closed systems have proved useful.[47] See, for example, the *Electronic Registration Act*:[48]

> 4. (4) 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.

See also the *Land Registration Reform Act* as amended:[49]

> 20. (2) A person shall not submit an electronic document unless the person is authorized to do so by the Director [of Land Registration].
>
> . . .
>
> 23. (2) A person shall not deliver an electronic document to the electronic land registration database by direct electronic transmission unless the person is authorized to do so by the Director.

Compare, as well, the Toronto electronic court filing pilot project, whose authorizing rule reads, ". . . a lawyer, or another person who has filed a requisition with the registrar, may use the authorized software to issue or to file electronically the following documents. . .".[50]

"Outsource" the signature

A third method of dealing with signatures in electronic communications systems is to "outsource" the storage of the signature, by making the signer hold on to the signature on paper while the governmental system gets an electronic equivalent. In case of dispute, the filer has to produce the manual signature. This system has been used for filing securities documents such as prospectuses, under the System for Electronic Document and Retrieval (SEDAR), operated by the Canadian Securities Administrators.[51]

The Toronto electronic court filing pilot project eliminated most signature requirements on material filed electronically, but for the key document, the affidavit of service showing the defendant had notice of the action, the filer was required to keep and produce on demand an original signed version of the affidavit.[52] The same technique has been used more recently for any signed document that is part of a proceeding subject to new electronic filing rules in designated areas of the

province.[53] Filing an individual federal income tax return electronically through an approved electronic filing service provider requires signing a document attesting to the accuracy of what is filed electronically; the agent keeps the signature until the tax authorities ask for it.[54]

Designate the technology informally

A further approach to signatures is to allow the Executive to use whatever technology appears satisfactory. For example, the *Compulsory Automobile Insurance Act*[55] permits the use of any signature approved by the Minister.[56] 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 applying electronically for renewal of one's licence plates. The government is, in effect, using a "click through" certificate with the electronic signature. By that time, the signer has already entered his or her plate number, insurance policy number and credit card number, so the chances of falsely denying signing the certificate of insurance are slim. (Driving an uninsured vehicle is a separate offence, so a successful denial of a signature at the kiosk could lead one into more trouble.)

A model of this kind of provision is the *Income Tax Act*,[57] which permits electronic filing of tax returns by "using electronic media in a manner specified in writing by the Minister [of National Revenue]". The specification spells out that using the three means of identification provided in the program constitutes the taxfiler's signature.[58]

Designate the standards for particular programs

Sometimes the use of electronic signatures is authorized expressly for particular statutes. An example is found in the *Provincial Offences Act* ("POA").[59] Amendments to the POA in 1993[60] allowed for electronic documents:

> 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.

The functional description of the electronic program is almost always left to regulations, since it requires more details than are usually put into statutes, the details may change as technology evolves, and frequently the responsible ministries do not know in detail what they want to do at the time the statute is enacted. The POA regulations are oriented more to function and less to technology than some.[61]

The regulation states:

> 1. A document is properly completed in an electronic format if the information provided,
>
> (a) is intelligible in a form prescribed under the Act when that information is used for any purpose under the Act; and
>
> (b) cannot be altered after the document has been signed electronically, except for the elaboration of coded information or its compression or encryption, or the addition of codes necessary for its proper submission to the Integrated Court Offences Network of the Ministry of the Attorney General.
>
> 2. (1) A document is properly signed in an electronic format if the document contains a code, name or number of a person that is capable of identifying the person as the originator of the document and the code, name or number,
>
> (a) is generated by electronic means at the same time as the document being signed or on completion of the document; and
>
> (b) is reasonably secure against unauthorized use.
>
> (2) A code, name or number is presumed reasonably secure against unauthorized use,
>
> (a) if the physical means of generating it are themselves protected; or
>
> (b) if the electronic means of generating it are themselves a secure code or if those means are protected by a password issued in confidence to the originator of the document.[62]

To date, these provisions have been used only for filing electronic speeding tickets issued under the photoradar system in 1994-1995. The photoradar program was discontinued before any of the provisions on the creation or signature of electronic documents was brought before a court for review.

Another recent example of defining electronic signatures is found in amendments to the *Ontario Business Corporations Act*.[63] Subsection 1(1) says:

> "electronic signature" means an identifying mark or process that is,
>
> (a) created or communicated using telephonic or electronic means,
>
> (b) attached to or associated with a document or other information, and
>
> (c) made or adopted by a person to associate the person with the document or other information, as the case may be.

This definition sets no standards of reliability at all. A requirement of, if not a standard for, reliability appears in the substantive provision:

> 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 the attorney, as the case may be.[64]

Two other notable examples of definitions of electronic signatures are found in the *Ontario Works Act, 1997*[65] and the *Ontario Disability Support Program Act*, 1997.[66] They contain the following provision on electronic signatures:[67]

> Where this Act or the regulations require an individual's signature, one or more of the individual's personal identification number (PIN), password, biometric information or photographic image may be used in the place of his or her signature to authenticate the individual's identity and to act as authorization of or consent to a transaction relating to an application for or the receipt of assistance.

This provision is currently not in use. Its form is modern and flexible. It will be necessary to spell out, no doubt in regulations, who decides when the provision comes into force and what particular method will be used in practice.[68] The individual welfare recipient will not be called on to make those decisions, though the language of the section appears to leave it open to any party to communications to do so.

Authenticating information coming out of government

The foregoing examples deal with authenticating documents coming into government, where the existing law has called for a signature for this purpose. The other task of authentication occurs for documents purporting to come from government, where the recipient needs to know with assurance that the document is official. Many legal documents contain official information that people can rely on to take action or change their legal position. Thus, this information has to be right. Current law recognizes this need through certificates and other documents that attest to their credible origins with some public institution. The documents are usually required to have some kind of evidence of their source, such as letterhead, seals or signatures of public officials. Some of these security requirements also tend to show that the information has not been altered since the issue of the documents. How is this to be done electronically?[69]

Define the problem away

A radical approach to this aspect of signatures is to define the problem away. A number of Ontario statutes simply say that a certificate of authority (e.g., identifying an inspector who has the right to enter premises to check them over) "purporting to bear the signature of the Minister" is admissible in court.[70] One understands the desire not to have to prove the Minister's signature or the authority to hold the certificate in every prosecution. However, such a form of self-authentication was not conceived for an era of electronic documents and arguably will not work well in the electronic world without further assurances of the information in the document.

Beyond this unpromising type of provision, two main methods seem to be developing, depending in part on the type of information at issue and its uses. The first is a reference back to some official and secure database. The second is the encryption of the documents, often in the context of a public key infrastructure.

Refer to secure source of data

We look first at the secure reference method. The Companies Branch of the Ministry of Consumer and Business Services creates corporations, which are bodies with special rules about liability. It is important for people to be able to know whether a particular organization is currently a corporation in good standing, and who its directors and officers are. The Companies Branch has always issued "Certificates of status" about corporations. It will also certify the names that appear on its register as directors and officers.

In recent years, the Branch has been issuing electronic certificates of this information. The certificates include a digitized signature of the Director of the Branch, i.e., an electronic representation that displays his/her handwritten signature. This makes a printout of the certificate look like the traditional document, but the electronic signature is worth nothing as security. Electrons can be moved from one document to another without detection (unless special measures such as encryption are used).

The real authentication feature in the electronic certificate is a "unique identifier" — a code that refers back to the official corporation file in the hands of the Ministry. Each certificate has a different identifier, so the certificate as well as the corporation can be identified. Someone who wants to check the validity of the information in a certificate can ask the Branch to provide information about the corporation so identified. The ease of checking the official information deters fraudulent alteration of the certificate by increasing the risk that such changes will be detected.

The Ministry of the Attorney General has recently established a similar system. People who win civil lawsuits are entitled to enforce their win by seizing and selling the defendant's property, within limits. The court issues a "writ of seizure and sale" through the office of the sheriff. This writ can also be registered against land held by the defendant, so money owed can be collected from the proceeds of any future sale of the land.

The writs and their registration against the land are now being done in electronic form.[71] The system must obviously ensure that the amounts seized, and the person from whom they are seized, are those named by the court in the judgment. This requirement is met by the use of a unique identifier that refers the electronic document back to the court file. Anyone needing to check the information can do so against the official record, and not have to trust the electronic document being presented at the time.

In addition, the writs are court documents. The *Courts of Justice Act*[72] requires that any document issued by the Court must bear the seal of the court. The Act also says that the Court shall have such seals as are approved by the Attorney General. While seals were originally impressions of particular forms on wax, and later on paper, their form has become much more flexible over time. The intention behind the mark is more important than its form, just as it is for signatures. The Attorney General has approved the unique identifiers as seals of the court for the purpose of the writs. Since these identifiers are unique to the document and link to a unique file, they provide better authentication than the physical seal, which simply identified the name of the

court, and could be imitated by someone with the means and incentive to do so.

The use of such unique identifiers to authenticate information depends on the reliability of the official database. Thorough security is needed to preserve that resource. The same is true of paper files, of course, and electronic files may be more secure than paper against loss or alteration, if they are properly managed.

While on the subject of seals, one may note the provision added to the regulations under the *Highway Traffic Act*.[73] The Electronic Documents regulation[74] says:

> 6. (2) In an electronic document or a printed copy of an electronic document, the seal of the Ministry may be represented by an asterisk.

This replaces one graphic symbol, a seal, with another graphic symbol, an asterisk. One understands the desire to escape an irremediably physical symbol with one that can be created electronically, but in doing so one loses the element of security given by the presence of the physical seal of the Ministry. There is no way to tell who created an asterisk. When this regulation was made, the use of unique identifiers had not been developed. That seems a better method of achieving the goals of the Ministry than the current regulation.

The federal government's legislation on electronic documents, the *Personal Information Protection and Electronic Documents Act*,[75] permits seals to be created electronically by use of what that Act calls "secure electronic signatures".[76] This term awaits regulations for its final meaning to become clear, but it appears likely that it will involve the use of encryption through the Government of Canada public key infrastructure. The next part of this paper discusses encryption techniques in more detail. For many government purposes, however, it is arguable that unique identifiers serve the same goal with considerably less complexity. It is a matter for debate which programs need encryption and which can rely on the simpler method.

Use encryption to sign documents

Some uses of legal documents do not permit a reference back to the database. Sometimes the identity of the person or the office sending the information is essential to its user. Where the document itself has to be traced, or its contents have to be secure on their own, then people may prefer to use encryption for authentication.

Encryption has been around for a long time to keep documents secret. If the key to the code is known only to two people, then the recipient of a coded message also knows who sent it.[77] For reasons beyond the scope of this paper, traditional encryption is not adequate for widespread use by large numbers of people. A relatively new form of encryption can be used for these purposes, and many public sector and private sector bodies are working to set up systems to use it.

Public key encryption uses two mathematically related keys to process documents. One key of the key pair encrypts, and only the other key of the pair will decrypt. Either one can do either task. If you know one key, you cannot figure out the other one. The principle of using public key cryptography is that one key (the "private key") of the key pair will be kept secret by its holder, and the other one will be made public (the "public key") to anyone who might need to know it. Anyone who holds the public key can read something encrypted with the private key. Only the holder of the private key can read something encrypted with the public key.[78]

This means that the use of a private key to encrypt is the equivalent of a signature in identifying the source of a document — only one person can have encrypted it.[79] There is also a way to use this technology to show that information has not been altered from the time it is encrypted to the time it is read.[80] While the mathematics of public key cryptography is well proven, its application in practice can be very complex, for administrative more than for technical reasons. It depends on very reliable identification of the holders of the private keys to the potential users of the system.[81] It also requires good key management, especially where large numbers of keyholders include those who retire or change positions or lose their private keys (which threatens to compromise the reliability of anything signed in the future with those keys). The system of software and hardware specification and rules of conduct of the parties is known as a public key infrastructure, or PKI.[82]

The Government of Ontario is building the "GO-PKI", and several ministries want to use it. Among them are Health, Community and Social Services, and the Justice sector ministries.[83] Some Children's Aid Societies are now using public key cryptography for secure electronic communications about vulnerable children. A number of policies and design features of the PKI remain to be developed. PKI is not a magic bullet, and one size does not fit all. Each user community will have to decide how to make the technology work for its members. It does seem to be the best form of electronic authentication for some programs. Some of these uses will work for information coming into government as well as for information going out.

At present, it seems likely that government uses of PKI in Ontario and federally[84] will not have special legislative authority, but it will be supported by a network of contracts, as are some of the electronic registration systems examined earlier in this paper.[85] Among those contracts may be "cross-certification agreements", by which PKIs of different governments, or of private sector organizations, agree to accept each others' certificates as the basis of reliability of the certificates on signatures from those systems. Such agreements depend on intensive technical and administrative controls, to justify the trust given to each others' practices.

Use a token of identity

In closing, one should note a non-signature method of authenticating a transaction. Traditionally, a person can be identified by one or more of three methods: what they are (e.g., biometrics or a handwritten signature), what they know (e.g., a password or PIN) or what they have (e.g., an ATM card or a physical key). The government of Ontario has announced[86] that it will issue for some provincial purposes smart cards — plastic cards with embedded processing chips — to help facilitate the administration of programs that depend on the identity and entitlement of individuals. A smart card could contain the representation of the cardholder's signature, or a representation of an electronic signature readily transmitted to the government's verification computer. It could, however, be treated as an authentication device without having to use the language of signatures at all. Electronic technology permits governments to expand their options to new forms of authentication, not just to new methods of doing the old things.

Just as the range of government services is broad, so too are the possible methods of authenticating information flowing in and out of government. Some methods present more legal challenges than others, and may need detailed legislative support. The options are starting to look more familiar than they were a few years ago, although it might be premature to consider them a "toolkit". More customization is needed than such a term implies.

Electronic Administration

The previous section of the paper has discussed legal issues presented by electronic service delivery, with particular focus on authentication through signatures or equivalents. We now look briefly at how electronic processes affect governments internally or in their relations with suppliers of goods and services.[87] In this respect, electronic administration resembles business-to-business (B2B) electronic commerce. Not all of these communications are strictly commercial in nature — for example, the relations of the government with its employees, who are often unionized — but the use of Internet protocols to format and communicate information, and the development of a less-hierarchical organization based on information sharing, are common between public and private sectors.

Government sometimes faces unique considerations when it goes electronic in this thorough way. The statutes dealing with administrative procedures, such as the *Financial Administration Act*,[88] assume that government ministries are stable and to a large extent self-contained. Sharing or delegating powers across departmental lines can be hard to understand for civil servants who are attentive to their authority. It is not the electronic communications as such that matter here — the replacement of paper is not the issue — but the lowering of structural barriers or supports.[89]

Likewise, as noted earlier, the *Freedom of Information and Protection of Privacy Act*[90] contemplates that "institutions" will keep personal information confidential according to the Act. Institutions are ministries of the government, not the provincial Crown as one.[91] Many government departments collect and use personal information. Their ability to share it or handle it in common is problematic under the Act.

The easy flow of information is not limited to a single level of government. Electronic technology permits the creation of databases and communications among levels of government as well. Federal, provincial and municipal governments can cooperate to cut their own costs, as well as to serve their populations better. At the limit, this can cause constitutional concerns: is the level of government legally responsible for action under the Constitution really performing it, or is the sharing of information and programs the equivalent of an impermissible intergovernmental delegation? These questions have scarcely begun to be asked, much less analyzed and answered.

The longest-standing example of cross-governmental cooperation, in the use of electronic communications for core administration, is the online procurement process. All levels of government use a system called MERX, which is a private organization run by the Bank of Montreal under contract to the federal and provincial governments, to provide online tendering services.[92] At present MERX makes public[93] requests for proposals and other invitations to tender. It does not provide a means for tenders to be submitted to government. The reasons for this are complex, and both practical and legal. How does one know where a bid comes from? (The authentication question again!) How does one prevent collusion among bidders? How does one guarantee that no bids will be opened before the appropriate time? Is a contract made online binding on the parties?[94]

The use of electronic communications can require substantial investments in hardware and software. Technology projects often seem to attract innovative methods of spreading the cost and the benefit of innovative programs. Governments get involved in "public private partnerships",[95] alternative service delivery, and outsourcing of all kinds. The benefits of such processes can be real, but close watch must be kept on the costs and allocation of income. Like public administration in any other medium, the possibilities for inappropriate operations require caution. The Provincial Auditor in Ontario has developed a close interest in some e-government projects for just these reasons.[96] In New Brunswick, such a partnership has led to litigation; the trial court found that the province had obtained the valuable benefit of learning "how not to attempt a complicated computer systems integration project".[97]

In addition, the Information and Privacy Commission has expressed concerns that involving the private sector in operating services for the government should not deprive the public of rights of access to information and protection of personal information that it would have if the government provided the services directly.[98] In practice, the province now has fairly standard contract terms to ensure that the responsibility for providing access and privacy is properly discharged.

Similar issues arise for the obligations of the government under the *French Language Services Act*,[99] when someone other than the provincial government itself provides the services. It may turn out that it is easier to provide at least information and sometimes transactions in both languages across the province by use of technology than it is in person. However, the government will need to ensure that outside contractors — in the private sector or other levels of government — do in fact provide full bilingual services in accordance with the Act.[100]

The practical and auditing aspects of electronic government we leave at this point, but the legal requirements will occupy us a bit longer.

Law Reform in Support of Electronic Government

Much of our law traditionally presumes the presence of paper in order to create or prove legal relationships. Private and public sectors have had to deal with the consequences of taking the paper away as communications and records have taken electronic form. It has been necessary to decide when one was using paper because the law required it, and when one was using paper because of the convenience of paper's qualities in use. Two simple examples illustrate the difference. Often in common law, an oral contract will bind the parties to it. Nevertheless, it is usual in higher-value transactions for the parties to "get it in writing". In law, a pencilled "X" may serve as a signature, for example on the will of an illiterate person. However, most people would not accept a cheque with a pencilled "X", in the signature line. What is "legal" and what is prudent may be different. People do an informal threat–risk analysis in deciding on the form of their everyday transactions, and often choose paper to express them.

Accommodation strategies

Where we have traditionally used paper, lawyers use a number of techniques to bolster the legal effect of using electronics.[101] Some work better for the private sector than for government; others are equally useful for both.

Contract

The oldest recourse of lawyers is probably contract: spell out the consequences of communicating with each other by electronic means. While this is most obviously appropriate where the parties are deciding on prudent practices only, it has an honourable history with legal requirements, too. The most important class of such contracts may be "trading partner agreements" between the parties to electronic data interchange (EDI).[102] EDI involves the use of formally structured computer communications for business purposes. Parties to EDI prescribe what they have to do to give legal effect to their communications. Trading partner agreements often say expressly that the communications are deemed to be in writing (and that agreement itself tends to be on paper), that signatures are to be done in a particular way, that specific records must be kept, and that evidence of transactions under the agreement will not be challenged because of the electronic form. Fortunately for the parties, but unfortunately for the law, very few if any trading partner agreements have come to litigation, so the validity of some of their provisions has not been definitively tested.

Technology

A second technique for resolving legal issues is the technology itself. Technology can control access to information, it can trace those who have had access to it, and increasingly it is able to offer methods of paying small amounts for individual events of access. The origin of electronic inquiries can be traced more and more. Where legal rights depend on such features of information, the rights are becoming more certain as the technology evolves.

Common law

A third technique of adaptation is the common law. The law changes as the society it serves changes. Just as it came to terms with telegram, telephone and telex, so now it is coming to terms with telecopiers (faxes)[103] and other forms of electronic communications. Judges know that documents are generated electronically, and sent and stored the same way. One sees this reflected in the law of evidence, where computer-generated records are almost never refused admission on the ground that they are unknown or unreliable by nature.[104] The words of the statutes will often be read in a way that accommodates these changes.

For example, what of the definition in the *Interpretation Act*[105] of "writing"? Subsection 29(1) defines it as follows:

> "Writing", "written", or any term of like import, includes words printed, painted, engraved, lithographed, photographed, or represented or reproduced by any other mode in a visible form.

Can this be understood to include computer communications? After all, the words that are visible on the

monitor's screen are usually made up of the symbols that we use for writing. While an argument can be made in this sense, the more common view appears to be that the definition aims at something more tangible. All the examples in the statute involve paper or an even more solid medium. Further, this argument does not extend to machine-readable documents that may well be useful for legal dealings, such as some EDI codes. Our courts have not been called on to answer the question, but many people have pushed for more certainty in the meantime.

Law Reform

The final recourse is to law reform: change the rule that requires paper, in one way or another. We have already noted some specific statutes authorizing the use of electronic records for electronic filing. Law reform has been of particular interest to government to resolve the question of electronic records. Government shares many of the concerns of the private sector in respect of electronic forms of information. Government enters into contracts, it relies on signatures, it seeks and produces original documents. It retains records, probably to a greater extent than anyone else.

However, the techniques of accommodation mentioned above are less available to government to resolve its concerns. For example, the government deals with most of its subjects without contract, so contractual remedies are of limited use.[106] Reliance on the development of the common law is also less satisfactory than for private interests, because individual cases apply only to the narrow facts of the case. Precedents and principles build slowly. Government needs broadly applicable legitimacy faster than common law developments often allow. It is therefore fair to say that government has had recourse more quickly than the private sector to law reform to satisfy these pressures in a way consistent with the obligations and culture described here.

Most of the early law reform in Ontario dealing with the use of electronic communications has thus applied to government uses, rather than to private sector transactions with other private sector bodies. Two additional reasons can be offered for this. First, government ministries have had access to the legislative process for their own programs and purposes, and have used that access to ensure the legal effectiveness of those programs. Private sector interests may not have had the same ability to focus the legislative priorities. Nothing improper is suggested here; the public interest in the legitimacy of government processes justifies this kind of priority in many cases.

Second, the power of public bodies to innovate may be more often in question than it is for private entities. Some public bodies are entirely creatures of statute, and have no more power than is expressly given to them by their governing law. Municipalities are in this class, as are many agencies, boards and commissions. Even where the limits are not so clear, there is comfort in knowing that the Legislature has turned its mind to the program's use of new media of communications and has allowed it.

This is not to say that the private sector is unaffected by the early reforms, only that it is the operation of government programs and registries that is usually at issue. We turn now to some examples.

Law reform to support particular programs

The following examples show different approaches to specific uses of information in electronic form. They often apply to electronic service delivery rather than electronic administration, because the legal rules applicable to providing services to the public are more likely than those governing internal processes to have language suggesting that paper is needed. We begin with reforms designed to support the use of electronic records for particular programs or types of program. This approach to reform has been reduced, though not eliminated, by the more generic approach described subsequently.

The general use of records, and in particular electronic records, has been authorized by statute in some cases. The *Public Guardian and Trustee Act*[107] was amended in 1997[108] to add the following section:

> 10.2. (1) The Public Guardian and Trustee may store information in any form or medium and may at any time transfer or re-transfer it to another form or medium, in whole or in part.
>
> (2) It is not necessary for the PGT to retain a record or an original document if the information it contains has been stored in some other form or medium.

One suspects that the drafters had in mind the potential to convert the voluminous documentation received on paper by the PGT to electronic images. Storage and record management are both easier in this form. One will note that this statute has no guidelines or standards relating to the techniques used to store or transfer information or the security of the records at any time.

Sometimes, the reforms have focused mainly on the use of electronic records in judicial proceedings. Here are some examples.[109] In the *Corporations Tax Act*,[110] subsections 93(6.1) to (6.3) provide that where information is filed electronically, the Minister may make printouts and the printouts are as admissible as the original information; certain electronic information may be extracted from electronically-filed information and that extract is admissible; and if the electronically-filed information is destroyed, a duly authenticated printout of it is admissible "and shall have the same probative force as the original return or document would have had if it had been proved in the ordinary way". These provisions ensure that the Minister's records may be kept electronically or on paper without affecting their admissibility in court if disputes arise with the taxpayers. Similar provisions have been added to other tax statutes.[111]

The 1997 amendments to the *Public Guardian and Trustee Act* referred to above[112] also included this section:

> 10.1. (2) A copy or print-out of a record of the Public Guardian and Trustee, authenticated in a manner approved by the Attorney General, is admissible in evidence and has the same probative force as the record (or the original document, if any, on which the record is based) would have had if the record (or the original document) had been proved in the ordinary way.

In this case, there is some control over formatting and security, in that the Attorney General has to approve the method of authentication. The Legislature has not limited the discretion of the Attorney General on this point, however.

We have already examined the law relating to electronic filing.[113]

Generic law reform

Much of this use-by-use, program-by-program, ministry-by-ministry law reform has been overtaken by more general legislation that solves most of the problems for most of the government, while doing the same for the private sector. This has the benefit of legislative economy and consistency across the government. It can also promote harmonization of legal principles across provincial and national borders, in times when communications make borders for some purposes almost meaningless. Much of the generic law reform in Canada and elsewhere is inspired by work of the United Nations, notably the *Model Law on Electronic Commerce of 1996*.[114] Within Canada, the Uniform Law Conference of Canada[115] prepared a uniform statute to implement the U.N. principles.

Uniform Electronic Commerce Act

The *Uniform Electronic Commerce Act* (UECA)[116] has been adopted by all the common law provinces in Canada and by the Yukon Territory.[117] This is comprehensive minimalist legislation, intended to make the law "media neutral", so the same rules will apply to records and communications in all media. It does not set up special rules for the electronic world. Instead, it sets out the ways by which electronic information can meet the standards that apply to all information, even though the standards have been expressed in words that suggest the use of paper. Despite its name, the Act applies to much more than commerce. It applies to all rules of law of the enacting jurisdiction, except where rules or transactions or documents have been expressly excluded.[118] Some provinces have given their statutes a broader name to reflect this reality.[119]

Governmental powers to use electronic records

The Act deals expressly with governmental powers to use information in electronic form. The UECA states:

> 17. (1) In the absence of an express provision in any [enacting jurisdiction] law that electronic means may not be used or that they must be used in specified ways, a minister of the Crown in right of [enacting jurisdiction] or an entity referred to in subparagraphs 1(c)(ii) [or (iii)] may use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with documents or information.
>
> (2) For the purpose of subsection (1), the use of words and expressions like "in writing" and "signature" and other similar words and expressions does not by itself constitute an express provision that electronic means may not be used.[120]

Electronic payments in and out of government are also expressly authorized.[121]

Principles of the Uniform Act

The Act is technology neutral — it does not say what technological means are to be used to comply with it. It aims at results and not at how they are achieved. It authorizes the use of "functional equivalents" to paper documents, i.e., electronic techniques that have the same function and satisfy the same policy objectives as the paper. Thus, for example, it provides that a requirement in law that information be in writing can be satisfied if the information is accessible so as to be usable for subsequent reference.[122] It says that if the law requires a signature, an electronic signature will suffice.[123] "Electronic signature" is defined as "information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document".[124]

> An electronic document may serve as an original if
>
> (a) there exists a reliable assurance as to the integrity of the information contained in the electronic document from the time the document to be presented or retained was first made in its final form, whether as a paper document or as an electronic document;
>
> (b) where the document in original form is to be provided to a person, the electronic document that is provided to the person is accessible by the person and capable of being retained by the person so as to be usable for subsequent reference; and
>
> (c) where the document in original form is to be provided to the Government,
>
> (i) the Government or the part of Government to which the information is to be provided has consented to accept electronic documents in satisfaction of the requirement; and
>
> (ii) the electronic document meets the information technology standards and acknowledgement rules, if any, established by the Government or part of Government, as the case may be.[125]

What is reliable is also described, in contextual terms:

> (2) For the purposes of paragraph (1)(*a*),
>
> (a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display;
>
> (b) the standard of reliability required shall be assessed in the light of the purpose for which the document

> was made and in the light of all the circumstances.[126]

Consent rule

From these examples, one can see that the Act takes a flexible approach to security, acknowledging that different uses and programs may have a different threat–risk analysis and need different assurances as to the source and integrity of the electronic communications and records. This puts a serious burden on users of electronic systems to think about what is prudent for them. The Act does not require anyone to use or accept documents in electronic form; this is spelled out expressly.[127] Anyone who feels insecure can refuse to deal electronically. The power to say "no" is the power to say "yes, if…", and to set specifications for electronic communications that will be accepted.

These consent rules are expressly extended to government,[128] which has an even stronger provision:

> Despite subsection (1), the consent of the Government to accept information in electronic form may not be inferred by its conduct but must be expressed by communication accessible to the public or to those likely to communicate with it for particular purposes.[129]

The reason for the stronger language is that government often does not have contracts with those who are communicating with it, so there is no opportunity to agree on standards, either for reliability or for compatibility with existing systems. Some people who communicate with government do so unwillingly, and they might be indifferent, at best, whether their communications did not work or even harmed the government's computers or data bases. Public sector consent must be explicit or express so that informal communications, such as a civil servant's e-mail, is not taken to be a ministry-wide consent to communicate officially by such means. It is arguable, however, that the recipient of electronic communications could rely on the apparent authority of the civil servant to use e-mail with legal effect. Express consent could be posted to a ministry Web site, or stated in other generally accessible media.

The definition of "public body" in Ontario, Alberta, and British Columbia, and "government" in the UECA, refers to particular ministries or departments, so that the express consent required for electronic communications is subdivided into these bodies. The consent of one ministry does not apply to another ministry, which may have different systems, or different demands for reliability.

Special safeguards for government

Beyond the general empowerment, and the restricted use of consent, the UECA contains special safeguards for government in the functional equivalence provisions. In general, these sections provide that besides meeting the general requirements of the sections, information coming into government in electronic form may be subjected to "information technology standards" set by the government.[130] Again, the definitions would allow such standards to be set by each department. The Act does not say how the standards are to be set, whether by regulation or simple decree or announcement.[131] To date, no province or territory has set any standards, as they all tend to accept information produced by most over-the-counter software, unless particular programs have special needs.[132]

Under the UECA principle, electronic information that flows out of government would be subject to the general functional equivalence rules to meet writing requirements. Only incoming information needs the protections from unusual or inadequate technology.

Special provisions in Ontario's legislation

Ontario's version of the UECA has some additional provisions inserted to provide comfort to the Information and Privacy Commission.[133] Alberta has followed suit in its legislation, sometimes in slightly different wording.[134] Two of the additional provisions affect government in particular. One is a reformulation of the consent provision to ensure that people will still be able to obtain government service in traditional ways — or at least that government will have to find other authority than this statute to go entirely online:[135]

> (4) Nothing in this Act authorizes a public body to require other persons to use, provide or accept information or documents in electronic form without their consent.[136]

The second ensures that the Act cannot be taken to reduce in any way the obligations to give access to electronic records, or to protect the privacy of individuals.

> 27. (1) Nothing in this Act limits the operation of the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, or any other provision of law that is intended to,
>
> (a) protect the privacy of individuals; or
>
> (b) provide rights of access to information held by public bodies and similar entities.
>
> (2) This Act does not authorize a public body or similar entity to destroy a document whose retention is otherwise required by a provision of law or a schedule for the retention or destruction of documents, where the document,
>
> (a) is in a non-electronic form; and
>
> (b) was first created by or on behalf of the body or entity, or communicated to it, in that non-electronic form.[137]

Subsection 27(1) no doubt reflects to some extent the concern of the Commission about externalizing electronic communications without provision for access,[138] since the literal terms of the Act otherwise would not lead one to believe that it was any threat to other statutes. The second subsection preserves the right to access documents in the paper form they originally were made in (if any), at least until they are destroyed in the normal course of record management. The government may not use the power to retain paper records in electronic form[139] to destroy prematurely paper records that are subject to access rights.

Implementation of the Uniform Act in Canada

In their legislation implementing the UECA, most provinces and the Yukon have kept the government provisions in the original form.[140] However, British Columbia is silent on government, except for receiving and making payments, trusting to the general consent provision to allow the government to protect itself and to impose standards as required.[141] Saskatchewan already had legislation about electronic filing,[142] so it brought that statute into its *Electronic Information and Documents Act*,[143] where it works a little differently. Manitoba has limited the operation of its functional equivalence sections to designated laws, but otherwise the government ("public body") rules are incorporated from the UECA.[144] New Brunswick has departed furthest from the UECA,[145] leaving exclusions entirely to the regulations, and not referring to government either. The views of officials in New Brunswick appear to be that these provisions are not necessary to achieve the desired results, but that the results will be the same in the end under their legislation.[146]

Other generic legislation

Quebec has not followed the uniform legislation, but its statute on documents created with new technologies aims to make Quebec's law media neutral, so that information will have the same legal effect regardless of the medium on which it appears, if it meets the basic requirements as to stability and reliability set out in the statute.[147] It does not deal expressly with government, on the principle that media neutrality subjects all users, public or private, to the same rules. Quebec's statute does have a consent provision, however, so no one can be compelled to receive documents in any medium other than paper.[148]

The federal government has adopted the *Personal Information Protection and Electronic Documents Act*[149] (commonly known as Bill C-6 or PIPEDA), of which Part 2 deals with electronic documents. The federal Act gives the government general power to use electronic documents where federal law does not specify a medium,[150] including receiving payments electronically.[151] Its functional equivalence provisions, however, apply only to provisions of federal law that are designated by regulation. Further, the government must at the time of designation make a regulation to say how the medium requirement is to be satisfied by an electronic document.[152] As of late 2001, no provisions of law have been designated, and no regulation announced.

The federal Act restricts the form of electronic signature in many circumstances, requiring that a "secure electronic signature" be used for signatures of ministers on certificates,[153] witnesses and witnessed documents generally,[154] affidavits,[155] and documents under seal,[156] to name a few. A secure electronic signature is partially defined in the Act,[157] but the details are left to regulation. The language of the Act suggests that the government contemplates prescribing digital signatures using certificates under the Government of Canada PKI,[158] but no regulations are yet public.

Legislation in many countries has followed the United Nations Model Law. Laws in the United States are similar to those in Canada, notably the *Uniform Electronic Transactions Act*[159] and the *Electronic Signatures in Global and National Commerce Act* (E-SIGN).[160] A review of such legislation around the world is maintained by several law firms.[161]

Legislation on electronic evidence

The remaining area for legislation of general application of interest to electronic government is the law of evidence. As noted earlier, courts have not had a very hard time admitting computer-generated records as evidence.[162] However, a number of theoretical difficulties present themselves in applying evidence law to electronic records, and some concern has been expressed that in the right or wrong case, a serious challenge could be brought to their admissibility.[163] Governments have an equal interest with the private sector in being able to enforce their legal rights in court, and thus with the admissibility of electronic records in judicial and administrative proceedings.

As a result, the Uniform Law Conference of Canada developed the *Uniform Electronic Evidence Act*[164] to deal especially with the "best evidence rule" that requires an original document to be presented or an explanation given why the original is not presented. Since electrons can be copied exactly, there is no difference among versions of an electronic document, and an "original" has no advantage in reliability over any copy. It is hard to know what an original is, as electronic records are produced. The *Uniform Act* turns instead to the reliability of the computer system from which the electronic record is produced.[165] A number of presumptions of reliability are provided in the Act,[166] and courts are expressly allowed to refer to applicable standards of reliability in making their determination.[167]

The *Uniform Act* has been adopted in Ontario, federally, and most other jurisdictions.[168] The *Civil Code of Quebec* has broadly similar provisions.[169] It will now be up to government, as well as the private sector, to keep their electronic records in conditions that will meet the relevant standards. The Canadian General Standards Board published in 1993 a National Standard on Microfilm and Electronic Imaging as Documentary Evidence.[170] Work is underway to supplement it with a general standard on electronic documents. A general and theoretical description of the criteria for reliable electronic records has been published by a working group at the University of Pittsburgh, with Canadian participation.[171]

Conclusion

The law applicable to electronic government is evolving quickly, on a framework of information technology and public expectations also in quick development. The narrow questions of the legal authority of government to use electronic communications are relatively easy, particularly as they are now expressly dealt with in enabling statutes based on the United Nations Model Law on Electronic Commerce.[172] Specific practices or relations with particular parties may require specific legislation in the future as in the past.

The main legal questions relating to electronic service delivery relate to authentication (including privacy) and the integrity of systems and documents. It is difficult to legislate with broad application on such subjects, for two reasons. First, the needs of users are different, even within government departments and programs. Second, the technology changes so quickly that laws based on particular hardware, software or configurations of them are likely to be out of date or too restrictive almost by the time they are enacted. Being first in the field may be an advantage in electronic commerce, but it is not obviously desirable in law reform. A process of acclimatization to the demands of the technology and an appreciation of what other means of adaptation may be available will give government some time to support their initiatives in a more appropriate way.[173]

Such caution is appropriate. The law cannot require what the technology cannot support. The law here is likely to be validating rather than normative. Until the right answers appear for questions of security and authentication, governments will be hard-pressed to make any conduct mandatory, beyond what is already provided. The ability of current law to provide answers to many questions of e-government should not be underestimated. When the gap between a flexible application of current law and the demands of new technology grows too great, then the legitimacy of e-government comes more severely into question. Different governments will have different views on when that point will be. They will need to find a way to act when it arrives.

Notes:

[1] *Uniform Electronic Commerce Act*, [1999] Proceedings of the Uniform Law Conference of Canada 380, online: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1, section 17.

[2] *Halsbury's Laws of England*, vol. 8(2), 4th ed. (London: Butterworth, 1986), Constitutional Law and Human Rights, para. 6(1).

[3] See, for example, *Ontario's Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. P.31, and the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56. The federal statute is the *Privacy Act*, R.S.C. 1985, c. P-21. Quebec is an exception in having had private sector privacy protection legislation since 1994: *An Act respecting the protection of personal information in the private sector*, S.Q. 1993, c. 17. The federal government's *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, came into force only in January 2001, for federally regulated activities. NOTE: Ontario statutes are online: http://www.e-laws.gov.on.ca. Federal statutes are online: http://laws.justice.gc.ca. For other Canadian legislation online, see http://www.acjnet.org/cdn_law/LegislativeMaterials.cfm. This article will not provide URLs for each citation of a provincial or federal statute.

[4] See, for example, the Electronic Commerce Task Force, Industry Canada, "Realizing the Opportunities" in *Canadian Strategy on E-Commerce* (December 2000), online: http://e-com.ic.gc.ca/english/strat/60_4.html. See also B. Krebs, "G8 Nations Mull Digital Divide Task Force Report" (1 June 2001, Washtech.com), online: http://www.newsbytes.com/news/01/166371.html. The United Nations has also been concerned. See Ross Shimmon, "From Digital Divide to Digital Opportunity" (December 2000, UNESCO), online: http://www.unesco.org/webworld/points_of_views/shimmon.shtml. There is now a journal devoted to analysing and overcoming the digital divide, the Electronic Journal on Information Systems in Developing Countries. It is online: http://www.unesco.org/webworld/news/000210_divide.shtml. Difficulties of access may arise from physical challenges as well as economic or cultural ones. The World Wide Web Consortium (W3C) has published guidelines in the context of its Web Accessibility Initiative for making Web sites accessible to those with physical handicaps: online: http://www.w3c.org/WAI. A number of countries, including Canada, are moving to ensure that at least public sites are suitably accessible.

[5] Ontario's access rules are also found in the *Freedom of Information and Protection of Privacy Act*, *supra* note 3, s. 10ff., and the *Municipal Freedom of Information and Protection of Privacy Act*, *supra* note 2. The federal legislation is the *Access to Information Act*, R.S.C. 1985, c. A-1.

[6] See, for example, the *Archives Act*, R.S.O. 1990, c. A.27.

[7] This issue is discussed in some detail in the Canadian Association of Law Libraries, *The Official Version: Proceedings of a National Summit to solve the problems of Authenticating, Preserving and Citing Legal Information in Digital Form* (Kingston: Canadian Association of Law Librarians, 1997), online: http://www.callacbd.ca/1997summit/index.html. See also National Archives of Canada, *The Keeping of Business Records for Law, Audit and Archives: A Report on the Experts' Meeting* (Ottawa, National Archives of Canada, 1999).

[8] Section 28 of the *Evidence Act*, R.S.O. 1990, c. E.23, provides that a record published in the *The Ontario Gazette* or the official gazette of Canada or any other province or territory in Canada is proof, in the absence of evidence to the contrary, of the originals and of the contents thereof. See also section 31.

[9] See Electronic Commerce Task Force, Industry Canada, "Government as a Model User", in Canadian Strategy on E-Commerce (December 2000), online: http://e-com.ic.gc.ca/english/strat/662.html.

[10] The Department of Justice (Canada) has published a useful checklist of legal issues presented by "government on-line", with links to official documents and statutes. It is online at http://canada.justice.gc.ca/en/ps/ec/gol.html. The categories of analysis are broken down differently from those in this paper but there is of course a substantial overlap of issues.

[11] Governments generally act only with the territory over which they have authority, and their publications aim implicitly and often explicitly at that territory and its residents. Thus, governments are probably less exposed than some private enterprises to the risk of furnishing content that offends the law in some of the places from which the information can be accessed. See the discussion of jurisdictional issues in the sources referred to, *infra* at 28.

[12] Canadian thinking on electronic service delivery is explored annually at the "Lac Carling" conference, organized by the Public Sector CIO Council. Papers from 2000 are at: http://www.itworldcanada.com/lac/events.cfm; http://www.oncecorp.com/presentations/index.html and http://www.policity.com/esd/subject/lac_carling.htm. See also the *Report of the Auditor General of Canada to the House of Commons*, Chapter 19, "Electronic Commerce: Conducting Government Business via the Internet" (Ottawa: Ministry of Public Works and Government Services, December 1998.)

[13] See, for example, the *Government Paperwork Elimination Act*, Public Law 105-227, Title XVII, for the United States. For Australia, see T. Worthington, "Future Directions in Electronic Service Delivery in the Public Sector" (Australian Computer Society, December 1998), online: http://www.acs.org.au/president/1998/past/pubit98.htm.

[14] R.S.O. 1990, c. P.10.

[15] See the *Land Registration Reform Act*, R.S.O. 1990, c. L.4, as amended by S.O. 1994, c. 27, s. 85(3).

[16] Online: http://www.gov.on.ca/CSS/page/services/fro/frohome.htm.

[17] Online: http://www.oeb.gov.on.ca/english/electronic_regulatory_filing.htm.

[18] Online: http://www.cbs.gov.on.ca/obc/english/4TJTBS.htm.

[19] Online: http://www.cbs.gov.on.ca/obc/english/4THKHN.htm.

[20] Online: http://www.cbs.gov.on.ca/Online_Services/english/index.htm.

[21] Online: http://www.gnb.ca/snb/e/index.htm.

[22] Online: http://www.ecitizen.gov.sg.

[23] Online: http://www.integratedjustice.gov.on.ca/.

[24] Online: http://www.lio.mnr.gov.on.ca.

[25] A computer security consultant recently described his inability to prevent juvenile hackers from closing down his system, and concluded that a stable Internet economy was simply inconceivable when 13-year-old children are free arbitrarily to deny Internet service with impunity. Steven Gibson, "The Strange Tale of the Denial of Service Attacks against GRC.COM", July 2001, online: http://grc.com/dos/grcdos.htm.

[26] One sometimes hears of "data authentication", which is proving integrity of a record, and "identity authentication", which is proving attribution of a record. Here we use "authentication" to refer only to identity authentication. We use it to mean checking identity, not adding identifying information to a document in the first place.

[27] John D. Gregory, "Electronic Legal Records — Pretty Good Authentication?" in Canadian Association of Law Librarians, *The Official Version*, *supra* note 7 at 61, online: http://www.callacbd.ca/1997summit/authjohngregory.html.

[28] For Canadian descriptions of the law, though mainly U.S. law, see Sookman, *Computer, Internet and Electronic Commerce Law* (Toronto: Carswell, 2000) at chapter 11; and Ogilvie Renault, "Jurisdiction and the Internet — Are Traditional Rules Enough?" (1998), online: http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4h. Also Michael Geist, "Is There a There There? Toward Greater Certainty for Internet Jurisdiction" (2001), online: http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf, which reviews the case law in detail. On public law jurisdiction, see Roger Tassé and Maxime Faille, *Online Consumer Protection: A Study of Regulatory Jurisdiction in Canada* (Ottawa, Office of Consumer Affairs, Industry Canada, 2001), online: http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4n.

[29] Schiff, *Evidence in the Litigation Process*, 3d ed. (Toronto, Carswell, 1988) at 728.

[30] See John D. Gregory, "Authentication of Digital Legal Records" (1999) 6 The EDI L.R. 47.

[31] The two functions are sometimes split out into "I&A" — identification and authentication. See National Institute of Science and Technology (US), "The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security", node 26, "Identification and Authentication", online: http://csrc.nist.gov/publications/nistpubs/800-11/node26.html.

[32] *Supra* note 3.

[33] The change in character of a public record when it becomes electronic, and particularly when it is connected to the Internet, presents dramatic challenges to traditional thinking, largely beyond the scope of this article. The Information and Privacy Commission of Ontario has published extensively on how to accommodate privacy concerns in using electronic records. A list of such publications is online: http://www.ipc.on.ca/english/pubpres/papers/summary.htm. The first regulation under the federal private sector privacy legislation, the *Personal Information Protec-*

tion and Electronic Documents Act, S.C. 2000, c. 5, dealt with disclosure of personal information already in a public record. Regulations Specifying Publicly Available Information, P.C. 2000-1777, 13 December 2000.

[34] Civil law jurists may take a different view. The Working Group on Electronic Commerce of the United Nations Commission on International Trade Law debated the contribution of signatures in determining integrity, in the context of preparing the Model Law on Electronic Signatures. The debate is reflected in reports of the Working Group's meetings, online: http://www.uncitral.org/english/workinggroups/wg_ec/index.htm, and in the (draft) Guide to Enactment of that Model Law, online: http://www.uncitral.org/english/workinggroups/ wg_ec/wp-88e.pdf at para 123. The final Model Law and Guide were adopted in July 2001. The Model Law is online: http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.

[35] A bit more unofficial detail on how these factors might work is set out in John D. Gregory, "Legal Situation of Electronic Signatures: an Ontario Perspective" (1999), online: http://www.euclid.ca/ontsig.html.

[36] *R. v. Fredericton Housing Ltd.*, [1973] C.T.C. 160 (F.C.T.D.).

[37] Jane Winn, "The Emperor's New Clothes: the Shocking Truth about Digital Signatures and Electronic Commerce" (2001) 37 Idaho L.R.353 at 367, online at http://faculty.smu.edu/jwinn/shocking-truth.htm.

[38] Chris Reed, "What is a Signature?" [2000 (3)] *Journal of Information, Law & Technology* (JILT), online: http://elj.warwick.ac.uk/jilt/00-3/reed.html.

[39] S.O. 1994, c. 32. The Act also provides legislative support for the Ontario Business Connects program discussed in the next part of this paper. The Act has been very influential elsewhere in Canada. Nova Scotia copied it almost verbatim into its *Business Electronic Filing Act*, S.N.S. 1995-96 c. 3, as did Newfoundland under the same title in S.N. 1997, c. B-12. Very broad statutes resting entirely on potential regulations were passed in 1998 by British Columbia — the *Business Paper Reduction Act*, S.B.C. 1998, c. 26 — and Saskatchewan — the *Electronic Filing of Information Act*, S.S. 1998, c. E-7.21, now repealed and made part of the *Electronic Information and Documents Act*, S.S. 2000, c. E-7.22.

[40] O. Reg. 442/95.

[41] This analysis and those that follow are based on the purpose of the system and not on any direct statements to this effect by Ministry officials.

[42] R.S.O. 1990, c. P.10.

[43] S.O. 1991, c. 44. The application of the general statute to particular regimes like that of the PPSA is authorized by regulation. See O. Reg. 75/92 for designation of the PPSA and and 759/93 for the *Repair and Storage Liens Act*.

[44] R.S.O. 1990, c. L.4, as amended by S.O. 1994, c. 27, s. 85, adding Part III on Electronic Registration, sections 17 to 32 inclusive.

[45] *Ibid.*, s. 21.

[46] For more information on electronic land registration, see online: http://www.teranet.ca/legal/teraview.html. The registration system also depends on complex regulations. See O. Reg. 16/99 (Automated System), 18/99 (Documents — General) and 19/99 (Electronic Registration).

[47] The contracts deal not only with technical standards but also with liability — or exemption from liability — for inauthentic, lost or mistransmitted messages.

[48] *Supra* note 43 at s. 4.

[49] *Supra* note 44 at ss. 20 and 23.

[50] *Rules of Civil Procedure*, R.R.O. 1990, c. 194 (made under the *Courts of Justice Act*, R.S.O. 1990 c. C.43), Rule 4.05.1(1), made by O. Reg. 488/99 s. 1.

[51] See http://www.sedar.com. The American system run by the Securities Exchange Commission, known as EDGAR, works the same way. See http://www.sec.gov/edgarhp.htm.

[52] *Ontario Rules of Civil Procedure*, *supra* note 50, Rule 16.09(6), made by O. Reg. 24/00 s. 5.

[53] *Ontario Rules of Civil Procedure*, *supra* note 50, Rule 4.01(5), made by O. Reg. 427/01 s. 4; *Rules of the Small Claims Court*, O. Reg. 258/98, Rule 1.06(8), made by O. Reg. 461/01 s. 2.

[54] See Part F of the Information Return for Electronic Filing of an Individual's Income Tax and Benefit Return, online: http://www.ccra-adrc.gc.ca/E/pbg/tf/t183eq/t183-01e.pdf.

[55] R.S.O. 1990, c. C.25.

[56] O. Reg. 278/95 says "a certificate of insurance required by subsection 13(1) of the Act may be in electronic form approved by the Minister of Finance." The approval itself is not on the public record, though it would be available under the provincial access to information legislation and probably without a formal application.

[57] *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.), s. 150.1.

[58] Netfile security guideline, online: http://www.netfile.gc.ca/security-e.html. The three identifying items are the filer's Social Insurance Number, birth date and Access Code provided by the Canadian Customs and Revenue Agency. The software from various private suppliers is tested and authorized each year, and listed online: http://www.netfile.gc.ca/software-e.html . The United States federal government has a similar rule, with self-selected PINs serving as signatures. See the Internal Revenue, press release, "2001 Filing Season Begins", IR-2001-1 (2 January 2001), online: http://irs.gov/efile/.

[59] R.S.O. 1990, c. P.33.

[60] The *Provincial Offences Statute Law Amendment Act*, S.O. 1993, c. 31, s. 1(27).

[61] The regulations were written with an eye on the United Nations Model Law on Electronic Commerce, *infra*, note 114, then in draft form. See John D. Gregory, "Electronic Documents in Ontario's Photoradar System" (1995) 6 J. Motor Vehicle Law 277. Related amendments were made to regulations under the *Highway Traffic Act* at the same time. See O. Reg. 499/94.

[62] The regulation goes on to describe how electronic documents may properly be filed by electronic transmission to the court offices.

[63] R.S.O. 1990, c. B.16, as amended by S.O. 1999, c. 12, Schedule F, s. 1.

[64] S.O. 1999, c. 12, Schedule F, s. 7(2).

[65] S.O. 1997, c. 25, Schedule A.

[66] S.O. 1997, c. 25, Schedule B.

[67] Section 76(1) of *Ontario Works* and subsection 57(1) of Disability Support.

[68] The provision about biometric identifiers raises matters of particular concern to the Information and Privacy Commission. See "Privacy and Biometrics" (1999), online: http://www.ipc.on.ca/english/pubpres/papers/pri-biom.htm.

[69] Not only information but also money may flow out of government, and government needs to be certain about who is receiving it. This is, however, an example of the earlier problem, authenticating inflowing information (claiming the right to payment), not the one where the recipient needs to know where information (in the form of a payment order) is coming from.

[70] See, for example, the *Industrial Standards Act*, R.S.O. 1990, c. I.6, subsection 15(2). There are over 50 such provisions in Ontario statutes.

[71] *Ontario Rules of Civil Procedure*, R.R.O. 1999 c. 914, as amended, Rule 4.05.1(2) and Rule 60(1.1).

[72] *Supra* note 50, s. 147.

[73] R.S.O. 1990, c .H.8.

[74] O. Reg. 499/94.

[75] S.C. 2000, c. 5, online: http://laws.justice.gc.ca/en/P-8.6/index.html.

[76] *Ibid.*, s. 39.

[77] Though proving to a neutral person which of the two keyholders sent the message may be more difficult, if that is put in question.

[78] Confidentiality can be ensured by using the recipient's public key — only the recipient, using the private key, can read what has been encrypted. Confidentiality and authentication are independent, however. One can digitally sign a document that is transmitted in plaintext, i.e., that anybody can read, but that nobody else can have signed.

[79] Generally, for a signature one encrypts a smaller text, a mathematical digest or "hash" of the document to be signed. This uses less computing power in the process, and also allows verification of the integrity of the digitally signed text. See the material cited *infra*, footnote 81. The intention of this "signature" in law remains a matter to be demonstrated from its context, like that of any other signature. The present discussion treats only of the technicality of attribution.

[80] The hash digest of the signed document is revealed when one verifies the signature. If the digest is the same as a new digest made by the recipient of the document, using the same hash function, then the document has not changed since it was signed.

[81] Nicholas Bohm, *Authentication, Reliability and Risks* (Meta-Certificate Group, 1997), online: http://www.mcg.org.br/auth_b1.htm. It will be advantageous for some people to pretend to be who they are not, i.e., to

claim to hold certificates or signing keys or to try to have them issued though they are not entitled to them.

[82] See John D. Gregory, "PKI in a (Small) Nutshell" (1999), http://www.euclid.ca/pkishort.html. More detailed explanations are at the Government of Canada PKI site, http://www.cio-dpi.gc.ca/pki/pki_index_e.html (accessed July 3, 2001) and http://www.pkilaw.com. The American Bar Association has recently published for comment detailed draft guidelines for evaluating PKI systems, online: http://www.abanet.org/scitech/ec/isc/pag/pag.html.

[83] Electronic filing of court documents over the Internet, authorized by the Rule cited *supra* note 52, will require the use of digital certificates based on a PKI. See the Integrated Justice e-filing web site, http://www.justiceontario.net

[84] See the Government of Canada site, *supra* note 82.

[85] Some other places do have legislation to support the use of digital signatures in a PKI, either for government uses or for public and private sectors alike. Principled discussions of such legislation are published by the Internet Law and Policy Forum, online: http://ilpf.org, especially the survey, http://ilpf.org/groups/survey.htm and the analysis, http://www.ilpf.org/groups/analysis_IEDSII.htm.

[86] See the Information and Privacy Commissioner's response to the announcements (April 2001), online: http://www.ipc.on.ca/english/pubpres/papers/smcard-e.htm. See also the IPC's "Smart Cards" (1993), online: http://www.ipc.on.ca/english/pubpres/papers/cards.htm, "Smart, Optical and other Advanced Cards: How to do a Privacy Assessment" (1997), online: http://www.ipc.on.ca/english/pubpres/sum_pap/papers/cards.htm, and "Multi-application smart cards: How to do a privacy assessment"(2000), http://www.ipc.on.ca/english/pubpres/papers/multiapp.htm.

[87] For a theoretical overview from a French perspective, see Georges Chatillon, "Les nouvelles procédures administratives de l'État" (2000) Colloque international, L'Internet et Droit: droit européen et comparé de l'Internet, online: http://droit-internet-2000.univ-paris1.fr/dossier8/Georges-Chatillon.doc.

[88] R.S.O. 1990, c. F.12.

[89] Recent amendments to Ontario's *Public Service Act*, R.S.O. 1990, c. P.47, have addressed some of these delegation challenges. *Public Service Law Amendment Act*, S.O. 2001, c. 7.

[90] *Supra* note 3.

[91] The term "institution" is defined in section 2 of the Act.

[92] For a general description online: http://www.merx.cebra.com/Services/AboutMERX/English/WM/WM_Default.asp.

[93] MERX makes offers public, but the details and the technical specifications are available only to its paid subscribers, which are businesses interested in doing contract business with governments.

[94] Legislation has answered that traditional question. See *infra* on law reform, text accompanying note 116.

[95] See the Canadian Council on Public Private Partnerships, online: http://www.pppcouncil.ca. Compare the Singporean approach, online: http://www.gebiz.gov.sg.

[96] Ontario Provincial Auditor, Report on Business Transformation Project/Common Purpose Procurement (MCSS), online: http://www.gov.on.ca/opa/english/e98/301.htm. Report on Project to Automate the Land Registration System (POLARIS), online: http://www.gov.on.ca/opa/english/en00/303eng00.htm. In fairness, it should be noted that large-scale information technology projects in the private sector as well are notorious for cost overruns and failure to achieve their objectives. J. Carroll, "The problem with big technology visions" (23 July 2001) Marketing Online Magazine, online: http://www.jimcarroll.com/articles/mktg15.htm. Other countries have similar concerns. In Australia, a Senate committee recently investigated government outsourcing agreements for information technology. Its report is online: http://www.aph.gov.au/senate/committee/fapa_ctte/ITOutsourcing/report/ITO%20accountability%20issues%20report.pdf.

[97] *Brunswick Data Inc. v. New Brunswick* (1998), 196 N.B.R. (2d) 263 (N.B.Q.B.), rev'd. (1999), 209 N.B.R. 196 (N.B.C.A.).

[98] See the IPC's 1999 Annual Report on contracting out, online: http://www.ipc.on.ca/english/pubpres/ann_reps/ar-99/ar-99e.htm#contract and recommendation number 5 in that Report, online: http://www.ipc.on.ca/english/pubpres/ann_reps/ar-99/ar-99e.htm#recommend. The Ombudsman has expressed similar concerns about the jurisdiction of that office over the private sector elements of such activities. See Ombudsman of Ontario, Annual Report 2000, p. 3, online: http://www.ombudsman.on.ca/pdf/EN-annualreport-2000.pdf.

[99] R.S.O. 1990. c. F.32.

[100] See, for example, *Commissioner of Official Languages v. Her Majesty the Queen (Department of Justice of Canada)*, 2001 FCT 239, online: http://decisions.fct-cf.gc.ca/fct/2001/2001fct239.html. This decision required the federal government to ensure that municipalities undertaking prosecutions under a federal statute must ensure full French language rights to defendants. The applicable law in this case was the *Official Languages Act*, R.S.C. 1985 (4th Supp.), c. 31, and the *Canadian Charter of Rights and Freedoms*, though provincial delegation legislation came under consideration too: the *Streamlining of Administration of Provincial Offences Act, 1998*, S.O. 1998, c. 4.

[101] See George Takach, "Internet Law: Dynamics, Themes and Skill Sets" (1999) 32 Can. Bus. Law J 1, and his book *Computer Law* (Toronto, Irwin, 1998), chapter 7.

[102] See Peter Jones, *EDI Law in Canada* (EDI Council of Canada, 1992); *EDI Council of Canada, Model Form of Electronic Data Interchange Trading Partner Agreement and Commentary* (EDI Council of Canada, Toronto, 1990); and Electronic Messaging Task Force of the American Bar Association, "The Commercial Use of Electronic Data Interchange — A Report and Model Trading Partner Agreement (1990)" 45 Bus. Law. 1645.

[103] Faxed proxies have been recognized as signed for the purposes of the corporations statute: *Beatty v. First Exploration Fund 1987 & Co.* (1988), 25 B.C.L.R.(2d) 377 (S.C.). Rules on when faxes are delivered (influencing where the contract was made) were stated in *Eastern Power v. Azienda communale energia* (1999), 178 D.L.R. (4th) 409 (Ont. C.A.) online: http://www.ontariocourts.on.ca/decisions/1999/September/eastern.htm. For a comment on this case and these themes, see John D. Gregory, *Receiving Electronic Messages* (2000) 15 B.F.L.R. 473.

[104] See, for example, *R. v. Bell and Bruce* (1982), 65 C.C.C. (2d) 377 (Ont. C.A., aff'd SCC). The question of evidence is dealt with again *infra*, text accompanying note 162.

[105] R.S.O. 1990, c. I.11.

[106] Contracts are at the base of several public information systems, however, such as the PPSA filings and the Toronto court e-filing pilot project, as described in the electronic service delivery section *supra* text accompanying notes 47–49.

[107] R.S.O. 1190, c. P.51, re-enacted by S.O. 1992, c. 32, s. 25.

[108] S.O. 1997, c. 23, s. 11(5), adding section 10.2 to the Act.

[109] More recent general reform of the law of evidence is noted *infra* in text accompanying note 161.

[110] R.S.O. 1990, c. C.40, as amended by S.O. 1994, c. 14, s. 42(2).

[111] The *Revenue and Liquor Licence Statute Law Amendment Act, 1993*, S.O. 1993, c. 18, amended these statutes with identical or similar provisions: the *Fuel Tax Act*, R.S.O. 1990, c. F.35 (s. 2(21) added ss. 18(4.1)ff); the *Gasoline Tax Act*, R.S.O. 1990, c. G.5 (s. 3(17) added ss. 16(5.1)–(5.3)); the *Land Transfer Tax Act*, R.S.O. 1990, c. L.6 (s. 4(21) added ss. 10(3.1)–(3.3)); the *Race Tracks Tax Act*, R.S.O. 1990, c. R.1 (s. 7(11) added ss. 2(5.1)–(5.3)); and the *Tobacco Tax Act*, R.S.O. 1990, c. T.10 (s. 8(12) added ss. 23(5.1)–(5.3)). See also the *Employers Health Tax Act*, R.S.O. 1990, c. E.11, ss. 26(2)–(4) added by S.O. 1994, c. 8, s. 24.

[112] *Supra* note 108.

[113] *Supra* text accompanying notes 50 and 52.

[114] *Official Records of the United Nations General Assembly, Fortieth Session, Supplement No. 17* (A/40/17), online at http://www.uncitral.org/english/texts/electcom/ml-ec.htm. The Guide to Enactment to the Model Law is a valuable source of commentary on these issues. It is at the same Internet address, given here, as the Model Law itself.

[115] The Uniform Law Conference of Canada is an organization sponsored by the federal, provincial and territorial justice ministries to promote harmonization of Canadian law. It has been in operation since 1918. More detail is available online: http://www.ulcc.ca.

[116] *Supra* note 1. The *Uniform Act* is annotated with the purpose of each section.

[117] For citations and URLs for all this legislation, see the implementation chart on the Uniform Law web site, http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4b.

[118] *Supra* note 1, s. 2.

[119] Saskatchewan has enacted the UECA as the *Electronic Information and Documents Act*, and British Columbia, Alberta, and New Brunswick have called it the *Electronic Transactions Act*, though it is broader than just transactions. See also John D. Gregory, "Canadian Electronic Commerce Legislation" (2002) 17 B.F.L.R. (No. 3), forthcoming, spring 2002.

[120] *Supra* note 1, s. 17.

[121] *Ibid.*, s. 18.

[122] *Ibid.*, s. 7. The rule is taken directly from Article 6 of the United Nations Model Law on Electronic Commerce, *supra* note 113. See paragraphs 47–52 of the Guide to Enactment of the Model Law on writing requirements.

[123] *Ibid.*, s.10.

[124] *Ibid.*, s. 1.

[125] *Ibid.*, s. 11(1).

[126] *Ibid.*, s. 11(2).

[127] *Ibid.*, s. 6(1).

[128] *Ibid.*, s. 1. Alberta, British Columbia, and Ontario use the expression "public bodies" rather than government. In 2002, Saskatchewan proposed to amend its legislation to the same effect: *Electronic Information and Documents Amendment Act, 2002*, second reading April 17, 2002, available at http://www.legassembly.sk.ca/bills/PDFs/bill-07.pdf.

[129] *Ibid.*, s. 6(2).

[130] UECA, ss. 8(*b*), 9(*b*), 10(3), and 11(3). Ontario rolled them up into two sections and put them into the part of the Act dealing with the powers of public bodies. *Ibid.*, ss. 16 and 17.

[131] The term "information technology standards" and the non-regulatory approach were inspired by Australia's *Electronic Transactions Act, 1999*, online: http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm, ss. 8–12.

[132] The Ontario government has, however, set detailed standards for Electronic Data Interchange (EDI) between the Ministry of Finance and businesses paying tax electronically. Such payments are made in high volume, especially for employer health tax remitted by companies that provide payroll services for many large employers. Alberta's *Electronic Transactions Act*, on the other hand, anticipates regulations on such standards in that province. S.A. 2001, c. E-5.5, ss. 21 and 23. The Alberta *Electronic Transactions Act* is not yet in force.

[133] *Electronic Commerce Act, 2000*, S.O. 2000, c. 17 in force October 16, 2000.

[134] *Electronic Transactions Act*, *supra* note 132.

[135] See, for example, s. 205.1 of the regulations under the *Income Tax Act* (Canada), C.R.C. c. 945, which requires any person filing more than 500 returns (such as administrators of estates or trusts) to file them electronically.

[136] *Supra* note 133, s. 15(4).

[137] *Electronic Commerce Act, 2000, Ibid.*, s. 27.

[138] *Supra* note 98.

[139] *Electronic Commerce Act, 2000*, *supra* note 133, subs. 12(1).

[140] See the implementation chart referred to *supra* at note 117.

[141] *Electronic Transactions Act*, S.B.C. 2001, c. 10, online: http://www.legis.gov.bc.ca/2001/3rd_read/gov13-3.htm.

[142] *Supra* note 39.

[143] S.S. 2000 c. E.7-22, online: http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/E7-22.pdf.

[144] *Electronic Commerce and Information Act*, S.M. 2000 c. E.55, online: http://www.gov.mb.ca/chc/statpub/free/pdf/b31-1s00.pdf.

[145] *Electronic Transactions Act*, S.N.B. 2001, c. E-5.5, online: http://inter.gov.nb.ca/legis/bills/54%2D3/070e.htm.

[146] See the consultation paper *Electronic Transactions Legislation*, New Brunswick Department of Justice, December 2000, which annotates the UECA section by section and recommends a legislative response or silence to each section. Online: http://www.gnb.ca/justice/electronic-ev.doc.

[147] *An Act to establish a legal framework for information technology*, S.Q. 2001, c. 32, online: http://publicationsduquebec.gouv.qc.ca/fr/cgi/telecharge.cgi/161A0129.PDF?table=gazette_pdf

[148] *Ibid.*, s. 29.

[149] *Supra* note 75.

[150] *Ibid.*, s. 33.

[151] *Ibid.*, s. 34.

[152] See, for example, *Ibid.*, s. 41. This "opt-in" formula was used in the UECA for government documents in the draft current in the summer of 1998, when the federal government was drafting what became Bill C-54 and then C-6. Online: http://www.ulcc.ca/en/poam2/index.cfm?sec=1998&sub=1998ja e.g., s.12.

[153] *Ibid.*, s. 36.

[154] *Ibid.*, s. 46.

[155] *Ibid.*, s. 44.

[156] *Ibid.*, s. 39.

[157] *Ibid.*, ss. 31 and 48.

[158] The GOC PKI is described online, see *supra* note 81. The language of s. 48 resembles "technology neutral" language first devised by the National Institute of Standards and Technology (NIST) in the United States in 1991 and frequently used in legislation in many countries since then, and in the European Union's Directive on Electronic Signatures of 1999, online: http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/1_013/1_01320000119en00120020.pdf. Almost nowhere has any method other than digital signatures been held to satisfy the standard, though California has decreed that signature dynamics would be acceptable too. California Digital Signature Regulations (1998), online: http://www.ss.ca.gov/digsig/regulations.htm.

[160] Public Law No. 106-229, 114 Stat. 464 (2000) (codified as 15 U.S.C. §§ 7001-7006, 7021, 7031) (enacted S. 761); available online: http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws

[160] Public Law No. 106-229, 114 Stat. 464 (2000) (codified as 15 U.S.C. §§ 7001-7006, 7021, 7031) (enacted S. 761); available online: http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws

[161] See, for example, the Baker and McKenzie site, http://www.bmck.com/ecommerce or the McBride Baker Coles site, http://www.mbc.com/ecommerce/ecom_overview.asp.

[162] *Supra* note 104.

[163] See, for example, Ken Chasse, "Computer-Produced Records in Court Proceedings" [1994] Proceedings of the Uniform Law Conference of Canada , online: http://www.ulcc.ca/en/poam2/index.cfm?sec=1994&sub=1994ac; Hamish Stewart, "Some Thoughts on Computer-Generated Evidence" [1996] Proceedings of the Uniform Law Conference of Canada 143, online: http://www.ulcc.ca/en/poam2/index.cfm?sec=1996&sub=1996aa.

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

[165] *Ibid.*, s. 4(1).

[166] *Ibid.*, s. 5.

[167] *Ibid.*, s. 6.

[168] See the implementation chart referred to *supra* note 117, which also notes progress for the evidence statute.

[169] Articles 2837–2839. Article 2837 was repealed and replaced by the recent Quebec statute on information technology, *supra*, note 147.

[170] CAN/CGSB-72.11-93, described online: http://www.pwgsc.gc.ca/cgsb/catalogue/specs/072/072_011-e.html.

[171] University of Pittsburgh, School of Information Sciences, Functional Requirements for Evidence in Recordkeeping (1995), online: http://web.archive.org/web/20000818163633/www.sis.pitt.edu/~nhprc/.

[172] *Supra*, text accompanying note 114.

[173] For example, the State of Utah's *Digital Signature Act*, Utah Code, s. 46-3, was innovative and thorough back in 1995, but it was much criticized on some of the grounds suggested here, and it has not been widely followed. Most states have enacted the *Uniform Electronic Transactions Act*, *supra*, note 159, instead.