COMMENT

Bill C–6: Federal Legislation in the Age of the Internet

MICHAEL POWER*

Many countries are developing strategies to meet some of the challenges of electronic commerce. But Canada is taking on all of them. Our bold and comprehensive vision will make it possible for Canadian business and consumers to seize the potential of E-com first, and fastest. We call our E-com strategy "The Seven Firsts." And most of it will be in place by the end of this year.

We will have privacy legislation to protect personal data, a policy on the use of encryption technology, and a world-class public key infrastructure in place.

New consumer protection guidelines will ensure that Canadians enjoy the same protection online that they do at the corner store.

We will table legislation that gives electronic signatures a basis in law.

A revenue-neutral taxation regime will ensure that you are not taxed twice.

And we will have standards that the world will follow.

–Jean Chrétien, St. John's Newfoundland, 22 September 1998.

I. INTRODUCTION

HISTORICALLY, THE INTERNET dates from 1968 and the World Wide Web from 1992.[1] Despite this recent beginning, the Internet and the Web

* Department of Justice Canada, currently seconded to Treasury Board Secretariat serving as Assistant Director, Policy, Interdepartmental PKI Task Force. The views expressed in this paper are the personal views of the author and do not necessarily reflect the views of the Department of Justice, Treasury Board or any other department or agency of the Government of Canada. The author wishes to thank Helen McDonald of Industry Canada and Joan Remsu and Robert DuPerron of Justice Canada for their thoughtful comments. Any errors or omissions remain those of the author.

are comparable to the invention of the printing press in terms of their effect upon society. Governments around the world recognise this fact and are preparing their economies for the impact of new communication and information technologies.[2] At the risk of overstating the matter, the country that best updates its legal framework to facilitate electronic commerce will gain a comparative economic advantage in the early part of the 21st century. Facilitating electronic commerce can mean a variety of things—this author argues that it should focus on establishing trust and building confidence in the electronic means by which people communicate and transact business.

A large part of building trust and confidence is to respect the privacy of information about users. Information about an individual is valuable because it can be used to target individuals in the marketing of goods and services. It is increasingly a commodity for purchase or sale. Protecting privacy used to be about controlling what government did with personal information because government, at one time, was the only entity that collected information about individuals on a large scale. The increasing use of powerful computers allows the creation and combination of databases of personal information, and the use of networks such as the Internet permits the easy transfer and sale of data across national borders. It is not surprising that these developments have been accompanied by growing concerns about privacy and a recognition that these concerns, if not addressed, will slow the take-up of electronic commerce.

Governments also have an interest in using the Internet as a means of providing service to its citizens. This raises legal issues with respect to whether government can realise the full potential of this new communication and distribution tool. Is there appropriate statutory authority? Are there questions of statutory interpretation? While these are general questions, one can move into the specifics very quickly. For example, do keystrokes which produce intangible electrons on a computer screen constitute a document *in writing* as required with respect to an application being made under Statute X?

---

1 The contract to develop the Internet was awarded in 1968. The physical Internet was built a year later. Marc Andreessen, the NCSA and the University of Illinois created the first graphical user interface for the world wide web in 1993. For a complete timeline, see D. Kristula, "The History of the Internet" (1997) online: <http://www.davesite.com/webstation/net-history.shtml (last modified: 1 March 1997).

2 See *e.g.* United States, The President's Information Infrastructure Task Force, *A Framework for Electronic Commerce*, (1997) online: <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (last modified (1 July 1997); Australia, National Office for the Information Economy, *Towards an Australian Strategy for the Information Economy* (1998), online: <http://www.noie.gov.au/nationalstrategy/index.html> (last modified: 29 July 1998); European Commission, *Europe at the Forefront of the Global Information Society: Rolling Action Plan*, (1997) online: <http://www.ispo.cec.be/infosoc/legreg/rollcomm.html> (date accessed: 30 September 1999).

On 1 October 1998, as part of the implementation of Canada's electronic commerce strategy, John Manley, Minister of Industry introduced Bill C–6[3] in the House of Commons. This comment provides a short introduction to the proposed legislation.

Bill C–6 addresses a number of subjects and is divided into five parts:

Part 1: Protection of Personal Information in the Private Sector
Part 2: Electronic Documents
Part 3: Amendments to the *Canada Evidence Act*
Part 4: Amendments to the *Statutory Instruments Act*
Part 5: Amendments to the *Statute Revision Act*

The legislation originally constituted two separate bills—Part dealing with data protection, and Parts 2-5 dealing with federal legislation. While Part 1 addresses more than just privacy in an electronic environment, thematically the two proposals are linked as part of the federal government's electronic commerce strategy and, as a result, were merged just prior to their introduction in the House of Commons.

II. Protection of Personal Information in the Private Sector

With respect to privacy, the federal government and most provinces have legislation governing the public sector's collection, use, and disclosure of personal information. However, outside of Quebec,[4] protection of personal information in the private sector is sporadic and uneven. The federal Information Highway Advisory Council (IHAC) studied the issue of privacy in 1995 and recommended the development of federal privacy legislation.[5]

---

[3] Bill C–6, *An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act*, 2nd Sess., 36th Parl., 1999, (3rd Reading 26 October 1999). As of the time of writing the bill was before the House of Commons, 1st Sess., 36th Parl. as Bill C–54. The Bill has since been re-introduced without change as Bill C–6. This comment discusses the text of bill C–54 as originally introduced.

[4] The Province of Quebec has comprehensive privacy legislation covering both public and private sectors.

[5] Canada, *Report of the Information Highway Advisory Council: Building the Information Society: Moving Canada Into the 21st Century* (Ottawa: Industry Canada, 1996).

There are also international concerns about the treatment of personal information. The European Union's *Directive on Data Protection*,[6] which came into effect on 25 October 1998, prohibits the transfer of personally identifiable data to third countries that do not provide an adequate level of privacy protection.

After consideration of all of these factors, the federal government responded with a process that began with the publication of a public consultation paper[7] and ended with the creation of Part 1 of Bill C–6.

Information privacy is the right of individuals to determine when, how, and to what extent they will share personal information about themselves with others. Part 1 is intended "to provide Canadians with a right of privacy with respect to their personal information that is collected, used, or disclosed by an organisation in an era in which technology increasingly facilitates the collection and free flow of information."[8]

Part 1 will initially apply to organisations in the federally regulated private sector, including telecommunications, broadcasting, banking, and inter-provincial transportation. It will not only apply to federal Crown corporations operating in these areas but also to federal entities which are not covered under the existing federal *Privacy Act*.[9] The provisions will also apply to trade in personal information that occurs inter-provincially or internationally where the information itself is the subject of the trade.

Three years after coming into effect, the provisions will apply more broadly to all personal information collected, used, or disclosed in the course of commercial activities, as well as to inter-provincial and international flows of personal information in the course of commercial activities generally. The law will not apply to:

(i) any non-commercial activities;
(ii) charities, universities, schools or hospitals;
(iii) the professions except where these organisations are engaged in commercial activities;
(iv) employee records in the provincially regulated private sector;
(v) agents of the Crown in right of the province; or
(vi) municipalities.

---

6 EC, *Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L. 281/1.

7 Canada, Electronic Commerce Task Force, *The Protection of Personal Information: Building Canada's Information Economy and Society* (Ottawa: Industry Canada, 1998)

8 Bill C–6, *supra* note 3 at s. 3.

9 R.S.C. 1985, Chap. P–21. Such federal entities include Canada Lands Co., Cape Breton Development Corporation (DEVCO) and Enterprise Cape Breton.

If a province adopts legislation that is substantially similar, the organisations, classes of organisations, and activities covered under Part 1 will be exempted from the application of Part 1. After any such exemption, the federal law will still apply to federal works, undertakings, and businesses, as well as to trans-border data flows of personal information.[10]

A. Privacy Principles

Section 5 requires every organisation subject to Part 1 to comply with the obligations set out in Schedule 1, which are the principles set out by the Canadian Standards Association in code Q830, *Model Code for the Protection of Personal Information*.[11] The standard, which was a consensus of industry, consumer and government on a set of fair information practices, outlines the means by which organisations should collect, use and disclose personal information and addresses the rights of individuals with respect to that information.

Schedule 1 of the Bill quotes ten principles from the national standard:

> Principle 1—Accountability
>
> An organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation's compliance with the following principles.
>
> Principle 2—Identifying Purposes
>
> The purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected.
>
> Principle 3—Consent
>
> The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.
>
> Principle 4—Limiting Collection
>
> The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means.

---

[10] See Bill C–6, *supra* note 3 at s. 4, para. 27(2)(d) and s. 30 with respect to the scope of Part 1. The constitutionality of such a provision is beyond the scope of this paper but suffice it to say that the federal government proceeded on the basis that it has the constitutional authority to act as it has.

[11] This standard was adopted by the Canadian Standards Association in 1996.

Principle 5—Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.

Principle 6—Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7—Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8—Openness

An organisation shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9—Individual Access

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10—Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organisation's compliance.

Schedule 1 may be amended by order of the Governor in Council to reflect future revisions to the National Standard.[12]

B. Exceptions

As with any rule, there are exceptions to provide the necessary degree of balance. In an open society like Canada's, some groups, such as law enforcement agencies and journalists, have a legitimate reason to collect, use, and disclose personal information without having to obtain the consent of the individuals concerned. As a result, Part 1 permits certain exemptions with respect to both collection and use.

---

[12] Bill C-6, *supra* note 3 at para. 27(2)(b).

Collection, without compliance with Part 1,[13] is permitted where:

(i) the collection is in the interest of the individual and consent cannot be obtained in a timely manner;
(ii) obtaining permission could infringe on the information's accuracy or prejudice the use for which the information is collected;
(iii) the collection, use, or disclosure is solely for journalistic, artistic or literary purposes.

Use of collected information is permitted without compliance with Part 1 where:

(i) where such information can contribute to the investigation of an offence;
(ii) the information is used in an emergency that threatens the life, health or safety of an individual;
(iii) the information facilitates the conservation of historically important records
(iv) the information is "collected" for purposes described in (1) and (2) above (i.e. for the individual's benefit; where the accuracy of the information is compromised; or where the use of the information would be prejudiced).[14]

C. Remedies & Audits

Division 2 outlines the remedies available under Part 1. Bill C–6 proposes a reactive, complaints-driven process.

Individuals will have the right to complain about any aspect of an organisation's compliance to the federal Privacy Commissioner who will have general powers to receive and investigate complaints and to attempt to resolve disputes.[15] If a dispute is unresolved with respect to specific matters, an application may be made by the complainant or the Privacy Commissioner, to the Federal Court for a hearing. In addition to any other remedy it may give, the Court may order an organisation to correct its practices or award damages to the complainant, including damages for any humiliation suffered by the complainant. Punitive damages may not exceed $20 000.[16]

The Privacy Commissioner may, on reasonable notice, audit the personal information management practices of any organisation if he or she has reasonable grounds to believe an organisation is contravening a provision of Division 1

---

[13] Bill C–6, *supra* note 3 at paras. 7(1)(a)–(c).

[14] *Ibid.* at paras. 7(2)(a)–(d).

[15] *Ibid.* at s. 11, 12.

[16] *Ibid.* at s. 14, 16.

or not following a recommendation set out in Schedule 1.[17] The audit findings may be included in the Commissioner's annual report to Parliament.[18]

III. ELECTRONIC DOCUMENTS

CONCERNS ABOUT THE INTERPRETATION of federal legislation in an electronic environment arose in 1995.[19] Following its establishment in 1996, the Electronic Commerce Secretariat at the Department of Justice began a review of federal legislation. The thrust of this review was to examine federal statutes that might contain language indicating a "paper-bias". Three hundred and thirty statues were found to contain such language or language where it might be uncertain that electronic alternatives were acceptable. As a result, given the range and number of statutes and regulations, the Department of Justice proposed a general approach in amending federal legislation. Part 2 is the result of that recommendation.

The purpose of Part 2[20] is "to provide for the use of electronic alternatives ...where federal laws contemplate the use of paper to record or communicate information or transactions."[21] Section 33, based in part on Section 18 of the *Department of Public Works and Government Services Act*,[22] is a general enabling provision confirming the authority of a Minister to use electronic means to deal with documents or information where he or she does not currently have the authority to do so.

A. Fees and Forms

To remove any possible confusion, s. 34 was placed in the text as a result of language dealing with the electronic payment of fees found only in the *Patent Act*.[23] If Parliament is silent in Statute A with respect to the same subject found Stat-

---

17 Bill C–6, *supra* note 3 at division 3, ss. 18 and 19.

18 *Ibid.* ss. 19(2) and 26(1).

19 See *e.g.* Canada, Department of Justice, *A Survey of Legal Issues relating to the Security of Electronic Information*, (1996) online: <http://canada.justice.gc.ca/commerce/ cover% 5Fen.html> (last modified: 15 November 1996), which included a recommendation, that the *Canada Evidence Act* or *Interpretation Act* be amended to ensure all federal legislation and programs have a common approach to the admissibility of electronic records.

20 Bill C–6, *supra* note 3 at s 31–51.

21 *Ibid.* s. 32.

22 S.C. 1996, c. 16.

23 Subsection 8(1) of the *Patent Act*, R.S.C. 1985, Chap. P–4, reads as follows:

> Subject to the regulations, any document, information or fee that is authorized or required to be submitted to the Commissioner under this Act may be submitted in electronic or other form in any manner specified by the Commissioner.

ute B, such an omission is generally interpreted to indicate that Parliament did not wish to act in the same manner in Statute A as it did in Statute B. The possible uncertainty resulting from the absence of other statutory provisions dealing with the electronic payment of fees suggested that this type of provision was appropriate. It should be noted that this deals only with the payment of fees *to* government. No similar provision is required with respect to payments *by* government since s. 35 of the *Financial Administration Act*[24] permits the government to make payments in an electronic manner, provided it is in a manner directed by Treasury Board.

The subject of electronic alternatives to forms and manners of filing is addressed in section 35. Subsections 35(1), (2), and (3) authorise a "responsible authority" to make regulations to provide for an electronic version of an *existing* form or an electronic manner of filing. Subsection 35(4) expands current powers under federal law to issue, prescribe or establish a form or manner of filing electronic documents or submitting information in an electronic form.

The concept of a "responsible authority" addresses the different relationships between federal entities and ministers responsible for statutes and regulations. Section 35 deliberately makes a distinction between "Acts of Parliament" and "federal law", the latter being broader and encompassing regulations.[25] Generally, a Minister is responsible for a provision of an Act of Parliament.[26] A minister may be responsible for regulations made pursuant to a statute but this is not always the case. In some instances, an arm's-length relationship is sought under legislation and regulations may be made by the Governor-in-Council or by a relevant agency. In one instance, a Minister is not responsible for the agency but only for the tabling in Parliament of the agency's annual report.[27] If for some reason, there needs to be a designation of a responsible authority for the purposes of Part 2, subsection 31(2) authorises the Governor on Council to designate a person or body as appropriate in the circumstances.

---

[24] R.S.C. 1985, c. F–11.

[25] Bill C–6, *supra* note 3 at s. 31(1).

[26] This can get complicated. For example, with respect to the *Access to Information Act*, R.S.C. 1985, c. A–1, the Minister of Justice is responsible for certain provisions while the President of the Treasury Board is responsible for the remainder.

[27] See *e.g.* the Public Service Commission; s. 47(1) of the *Public Service Employment Act*, R.S.C. 1985, c. P–33.

B. Secure Electronic Signatures

In some statutes, there exist provisions that permit certificates and documents signed by a minister or official to be entered into evidence.[28] Section 36 provides for electronic versions of such documents provided they are signed with the relevant person's secure electronic signature. At this point, it is appropriate to turn to a brief discussion of technology.

A number of sections in Part 2 accept the use of secure electronic signatures. Subsection 48(1) permits the Governor in Council, on the recommendation of Treasury Board, to make regulations prescribing technologies or processes that, in essence, constitute what the federal government would recognise as secure electronic signatures.

One must remember that an electronic signature can be a variety of things: a scanned hand-written signature, some letters at the bottom of an email message, etc. All of these can be manipulated since they are only digitised bits on a screen. A secure electronic signature is different in that it must:

(i) be unique to the individual in question;
(ii) be under that person's sole control;
(iii) be used to identify the person using the technology or process; and
(iv) linked to the document to which it is appended in such a way that the signature can be used to determine whether the document has been changed.[29]

The only technology that the federal government believes satisfy these requirements in 1998 is public key cryptography. The term secure electronic signature is used to recognise that other technologies may, in the future, meet these requirements.[30]

A comprehensive discussion of such technology is beyond the scope of this paper. As a very brief introduction to the subject, the reader should know that public key cryptography encrypts information by using two mathematically related keys: one is kept private, the other is made public. The private key cannot be determined from the public key. An individual who wants to send a message uses the public key of the recipient to encrypt the message. The recipient uses

---

[28] A simple example is s. 14(1) of the *Fish Inspection Act*, R.S.C. 1985, c. F–12:

> Every inspection certificate is evidence of the facts stated therein and is admissible in evidence without proof of any signature or the official character of any person appearing to have signed it.

[29] Bill C–6, *supra* note 3, at the criteria listed in subsection 48(2).

[30] One can see other forms of cryptography on the horizon. Tests to manipulate randomly generated photons to produce "quantum cryptographic keys" and transmit them via satellite have been successfully completed. See "Encryption Advance For Secure Global Communications", Associated Press, 7 October 1998.

his or her private key to decrypt the message. The sender therefore knows that only the intended recipient can read the message.

Public key cryptography can also be used to create digital signatures. A digital signature is made when a mathematical function creates a unique summary of, for example, a message, which is then attached to the message and encrypted using the sender's private key. The recipient of the message can decrypt the digital signature using the sender's public key. The recipient then passes the message through the same mathematical function to produce a second summary of the message. If the digital signature can be decrypted and the summaries are identical, then the recipient is assured of both the sender's identity and the integrity of the message—meaning the message was not altered from the moment it was digitally signed. Because a unique digital signature is assigned to an individual, that individual's ability to repudiate a document is reduced.

This ability to verify the integrity of an electronic document is significant from an evidentiary point of view. Prior to the use of digital signatures, electronic documents were always subject to the question "how does one know that the document has not been changed?" Public key cryptography provides a method of determining whether or not a change has been made. One will not know what change has been made—only that the document differs from its original form. This integrity aspect of digital signatures is relied upon in several provisions of Part 2.

C. Electronic Alternatives

Governments retain documents or require the retention of documents. Section 37 recognises that the retention of an electronic document satisfies any existing requirement to retain records, subject to certain qualifications. These qualifications relate to preserving the ability to use the information in a retained document. In an electronic environment, there are different document formats or encryption programs that could frustrate the purpose of retaining the record in the first place. For example, one could retain an encrypted and unreadable document and arguably meet a record retention requirement. This section requires that the electronic document must be retained in its original format or, if converted, retained in a format that does not change the information in the document; the information is readable or perceivable to a person entitled to request the document; and any particulars (e.g. header information) is also preserved.

There are a number of references in federal legislation to notarial acts.[31] Under s. 38, a document that is recognised as a notarial act in the Province of Quebec is deemed to include an electronic version of the document if the elec-

---

[31] See, *e.g.* "notarial will" in s. 96(1)(b) of the *Bank Act*, S.C. 1991, c. 46.

tronic version itself is recognised under the laws of Quebec as valid and the federal law or its relevant provision is listed in Schedule 2 or 3.

This provision is the first to introduce Schedules 2 and 3. The global approach used in Part 2 demands a check and balance mechanism because there may be a valid reason for the retention of a paper-bias in a particular statutory provision. At the most basic level, considering not only the statute but also any international or inter-provincial obligation, it may have been the intent of Parliament to require something to be on paper or there may be a need to retain a paper-requirement. A second reason is that government may not be ready to accept electronic alternatives. One should note that the use of electronic alternatives requires a department (any department at any level of government) to re-engineer a business process, which takes time to implement properly. For both these reasons, the mechanism preventing the automatic application of a permission to use an electronic alternative is a requirement that the relevant provision be listed prior to the granting of that permission. Statutes are to be listed in Schedule 2 and regulations listed in Schedule 3.

Section 39 begins a series of equivalency provisions: a requirement for something is satisfied with an electronic something. In section 39, a requirement under federal law for a person's seal is satisfied by the use of a secure electronic signature that has been identified as a seal. Historically, one role of a seal has been to authenticate the identity of a person. A properly issued and valid digital signature performs the same function. How can a signature be a seal? The public key certificates, which provide evidence of digital signatures, contain distinguished names to establish their assignment to a unique individual, device or entity. A distinguished name, or DN, can simply identify the signature as a seal. Person X could sign and seal a document by applying two digital signatures: one bearing the DN of X, the other with a DN reading X-personal seal.

Legislation not only addresses how citizens and others deal with government but also how they deal with each other. Most legislation of this nature exists at the provincial level but provisions do exist at the federal level.[32] If such a provision does not contain a requirement referred to in sections 41 to 47 then section 40 may apply. For example, if there is a provision in a federal law requiring Person A to provide a document or information to Person B then that requirement is satisfied when Person A provides the document or information in an electronic form. This is subject to three conditions. The provision has to be listed in Schedule 2 or 3; both Person A and Person B have to agree that the document or information may be given in an electronic form; and the document given to Person B has to be under the control of Person B and usable for later reference. Arguably, a document that sits on Person B's C drive would be under his or her control; one that sits on Person A's web server would not.

---

[32] For example the *Bank Act*, S.C. 1991, c. 46, and supporting regulations require a bank to provide each customer with an account agreement in writing.

Requirements for a document to be in writing are satisfied by the use of an electronic document provided the relevant provision is listed in the appropriate schedule and the regulations respecting the application of this section has been complied with. With these conditions, the concept of compliance with regulations is introduced.

D. Regulations

The proliferation of formats in an electronic environment complicates planning for service delivery. Without reference to some controls, Part 2 would permit electronic alternatives to paper—any kind of alternative—and raise a host of new issues. No matter how much it might like to, government cannot yet provide service via every electronic means of doing so. Without some means of controlling how, when or where it will accept electronic documents, a responsible authority could be placed in a position where it could not refuse to accept a document in a format it is incapable of processing or which violates a substantive federal requirement found in a statute or regulation.

For example, a department could re-engineer a business process and provide, for example, web-based service to its clients.[33] It did so because the vast majority of its clients wanted to use the web to do so. For those who did not want to use the web, it could set up a system to receive documentation via e-mail. However, Person X could arrive at the government offices with a 5¼ inch floppy diskette and successfully argue that the government had to take it because it was in an electronic format and the legislation permitted its acceptance. The reference to regulations is intended to serve principally, but not exclusively, as a format and delivery control mechanism. For the balance of this paper, such regulations will be referred to as format regulations.

This regulation-making power is found in Subsection 50(1). Subsection 50(2) provides some guidance to a responsible authority as to the kinds of regulations contemplated. These include:

(i) specifying the technology or process to be used;
(ii) the format of an electronic document;
(iii) the place where a document is to be made or sent;
(iv) the time and circumstances when an electronic document is considered to have been sent or received; and
(v) the technology or process used to make or verify an electronic signature.

Where a responsible authority may not wish to make regulations but is required to do so—as in the case of the exchange of documents between Person A and Person B, under sections 40 to 47—then subsection 50(3) permits the creation

---

[33] An example is the filing of applications for review and notifications under the *Investment Canada Act* R.S.C. 1985, c. 28 (1st Supp.). Such filings may now be done over the web.

of minimum rules. These minimum rules provide that both persons have to agree to the electronic format and the document has to be under the control of the recipient and readable under subsection 50(4). Technical standards or specifications may be incorporated by reference into regulations.[34]

E. Originals and Signatures

Subject to specific conditions, section 42 permits the use of an electronic alternative where there is a requirement for a document to be an original. The reader has already seen two of the conditions: listing and compliance with any format regulation. The third condition is a requirement for a secure electronic signature to be added when the document was generated in its final form and which can be used to verify that the document has not been altered since that time. This third requirement relies on the integrity aspect of public key cryptography discussed above.

Subject to sections 44 to 46, an electronic signature satisfies any requirement in federal law for a signature. As noted above, a responsible authority may specify by regulation what type of electronic signature it will accept. The object is not to inhibit responsible authorities from making the technology or business process choices that, for sound business reasons, they may wish to make. However, in certain situations, an electronic signature will not be sufficient. Those situations involve requirements for signatures on sworn statements; certificates and witnessed statements.[35] The nature of the document; the need to have assurances as to the identity of the individual involved and the need for assurances as to the document's integrity dictate, within the confines of known technology, that a secure electronic signature be affixed to such documents. These classes of documents are also subject to the listing and format regulation requirements before electronic alternatives are acceptable.

Finally, requirements for multiple copies in an electronic environment are somewhat anachronistic. Does Person A hit the send button twice for duplicates and three times for triplicate copy requirements? Section 47 addresses the issue by stating that requirements for one or more copies are satisfied by an electronic document, provided, once again, that the document is listed and any format regulation is satisfied.

Two last points to note about the listing of provisions in the Schedules. First responsible authorities have the flexibility to add or remove provisions to a Schedule.[36] This recognises the concept of going off-line temporarily where a particular technology or process may not work as intended and may need to be replaced or upgraded. While this is done, the use of electronic alternatives may

---

[34] Bill C–6, *supra* note 3 at s. 50(4).

[35] *Ibid.* at s 44–46.

[36] *Ibid.* at s. 49.

be problematic and so it may be helpful to de-list a provision and then re-list when the technology or a particular aspect of it is replaced. If a provision is de-listed, the validity of anything done in compliance with any format regulation while the provision was listed is not affected.[37]

IV. AMENDMENTS TO THE *CANADA EVIDENCE ACT*

THERE ARE THREE TYPES OF AMENDMENTS to the *Canada Evidence Act*[38] in Part 3[39]. One deals with making various document-related provisions media-neutral; the second concerns work done in recent years within the Uniform Law Conference of Canada (ULCC); the third is related to secure electronic signatures developed in Part 2.

A. Published vs. Printed

The first type of amendment makes all the same changes to the *Canada Evidence Act*. They replace the term "printed" with the word "published". This is intended to remove the paper-bias associated with the word "printed" and permit the recognition in evidence of electronic versions of statutes, imperial documents, and regulations, orders and notices made by (1) the Governor General, Governor in Council and Ministers or (2) a Lieutenant Governor, or Lieutenant Governor in Council or head of any department in a province.[40]

The same thing is done with respect to notices, advertisements and documents found in the Canada Gazette. If published in an electronic version of the Canada Gazette, such items are admissible as proof, in the absence of evidence to the contrary, of the originals and of their contents.[41]

B. Uniform Electronic Evidence Act

Concurrent with federal work in the area of privacy and federal legislation, efforts were underway in the Uniform Law Conference of Canada (ULCC) to address the subject of electronic evidence.[42]

The ULCC recognised that courts have struggled with reliability within the confines of the traditional rules of evidence. With respect to electronic docu-

---

37 Bill C–6, *supra* note 3 at s. 51.

38 R.S.C. 1985, c. C–5.

39 Bill C–6, *supra* note 3 at s. 52–57.

40 *Ibid.* at s. 52–55

41 *Ibid.* at s. 57.

42 This work has been underway since 1993. See the Uniform Law Conference of Canada's web site at http://www.law.ualberta.ca/alri/ulc for extensive background material related to the ULCC's electronic evidence project.

ments, the term generates confusion in any consideration of authentication, best evidence, hearsay and weight.

Briefly stated, the best evidence rule requires a party to a dispute to produce the best evidence available. Generally this means an original paper document or the closest a party can get to one. The object is to obtain the most reliable evidence or the evidence with the best integrity. However, one must remember that the concept of original does not exist in an electronic environment. Except in situations where digital signatures are used, the integrity of an electronic document can be challenged because a change in an electronic document is harder to detect than in a paper document.

With increasing use of the Internet, this poses *real world* concerns. Electronic documents may become the norm rather the exception[43] and the greater use of imaging technology, in light of the storage cost of paper records, raises concerns that parties to a dispute may not be able produce records suitable for use in court. The ULCC's approach was to link the integrity of an electronic document to the reliability of the computer system that generated it. Evidence related to the latter helps determine the former.

The efforts to remove these concerns culminated in the adoption of the Uniform Electronic Evidence Act at the ULCC's 1998 Annual Meeting. Most of Part 3[44] enacts the substance of the ULCC Electronic Evidence Act.[45]

In Part 3, the burden of proving the integrity of an electronic document is on the person seeking to introduce it.[46] The best evidence rule is satisfied on proof of the integrity of the electronic documents system or if the evidentiary presumption related to secure electronic signatures applies.[47] A document-keeping system will be presumed to have produced a reliable electronic document if the computer system that generated it was working properly or, if not working properly, did not affect the electronic document and there are no other

---

[43] For readers that consider this extremely speculative, the author would remind them that twenty years ago the personal computer did not exist. Ten years ago, references to Universal Resource Locators did not appear in advertisement as they do now. Current generations may like the "feel" of paper but one ought to not extrapolate existing preferences to future generations.

[44] Section 56 of Bill C–6, *supra* note 3, adds sections 31.1–31.8 to the *Canada Evidence Act*. References hereafter will be to new, added sections.

[45] In December 1998, Ontario was the second jurisdiction in Canada to introduce legislation to enact the model evidence legislation. The model Act was section 7 of Schedule B to the *Red Tape Reduction Act*, 1998 (Number 2), Bill 101, which received first reading on December 15, 1998 but which died on the Order Paper on December 17, 1998, when the House rose.

[46] *Canada Evidence Ace, supra* note 38 at s 31.1.

[47] *Ibid.* at s. 31.2(1).

reasonable grounds to doubt the integrity of the document.[48] Integrity can also be established where the document was generated by a party adverse in interest or by a third party in the ordinary course of business.[49]

Affidavit or oral evidence may provide proof of reliability of a document-keeping system or the source of an electronic document.[50] Such evidence would be subject to cross-examination[51] that arguably would inspire information holders to carefully keep records and would hold parties accountable for claiming system reliability in the first place.

In considering the admissibility of an electronic document, a court may consider any standard, procedure, usage or practice concerning electronic document keeping.[52]

As indicated by the new section 31.7, nothing in these sections affects any rule of law related to the admissibility of documents, except the rules relating to authentication and best evidence. The thrust of these changes is to provide a threshold for judicial consideration of electronic documents by avoiding the search for an "original" and providing courts with the authority to consider the integrity of the system that generated the record.

It should be noted that a printout, when used as a paper document, satisfies the best evidence rule if it has been relied upon or used as a record of the information contained in the printout.[53] This may seem confusing but it reflects the usage and age of a printout and its "transformation" into a reference document.

C. Secure Electronic Signatures: Presumptions

The Uniform Electronic Evidence Act does not address the subject of secure electronic signatures. Bill C–6 does.

To better provide public administration, deliver services and communicate securely, the federal government is actively developing a public key infrastructure to facilitate the use of digital signatures as a type of secure electronic signature.[54] While provincial governments are now exploring how to use this technology for their activities, it was thought premature to include such presumptions in the model Act when, at the time, they were only of interest to the

---

[48] *Canada Evidence Ace, supra* note 38 at para. 31.3(a).

[49] *Ibid* at paras. 31.3(b) and (c).

[50] *Ibid* at ss. 31.6(1).

[51] *Ibid* at ss. 31.6(2).

[52] *Ibid* at s. 31.5.

[53] *Ibid* at ss. 31.2(2).

[54] For more information about the Government of Canada Public Key Infrastructure, visit the web site of the Interdepartmental PKI Task Force at http://cio-dpi.gc.ca.

federal government. Accordingly, because of its familiarity with the technology, the federal government proceeded with the inclusion of section 31.4.

Section 31.4 provides the Governor in Council with the authority to make regulations establishing evidentiary presumptions with respect to electronic documents signed with secure electronic signatures. The rational for this is simply that it is difficult to place presumptions in a statute about a technology that is unknown at the time of enactment of the statute. As technologies are determined to meet the criteria in subsection 48(2) and prescribed pursuant to subsection 48(1), only then can the subject of evidentiary presumptions be considered. This is not to suggest that presumptions will be created for each technology prescribed. But if it is determined that the creation of presumptions would be appropriate, then they can be put in place without the need to amend the *Canada Evidence Act*.

The types of regulations contemplated concern the association (or identification and linkage) of a person to a signature[55]; the integrity of a document signed with secure electronic signatures[56]; and the manner in which they be proved.[57] The *Canada Evidence Act* definition of secure electronic signature is the same as found in Part 2.

V. AMENDMENTS TO THE *STATUTORY INSTRUMENTS ACT*

PART 4, CONSISTING OF SECTIONS 58 AND 59, makes two amendments to *the Statutory Instruments Act*[58].

The most important of these amendments is a new provision that authorises the Governor in Council to determine the manner in which the *Canada Gazette* is published, including publication by electronic means. This change makes the *Statutory Instruments Act* consistent with other provisions in Parts 3 and 5 concerning publication of documents by electronic means.

An unofficial version of the Canada Gazette is available on-line now[59] but this amendment would, in effect, permit an "official" on-line version. The practical difficulties of ensuring document integrity and authentication remain. Is that really the document the Canada Gazette published on the web? Has any hacker tampered with the document since it was posted? These concerns are real given that both lawyers and judges could rely on the on-line version for research and argument. However existing security mechanisms coupled with

---

55 *Canada Evidence Act, supra*, at para. 31.4(a).

56 *Ibid.* at para. 31.4(b).

57 *Ibid.* at para. 31.4(c).

58 R.S.C. 1985, c. S–22.

59 See the *Canada Gazette* at http://canada.gc.ca/gazette/gazette_e.html.

digital signature technology present a means by which these problems can be addressed. The limitations in technology which prevented an official version of the Gazette are disappearing.

The second amendment in Part 4 amends subsection 16(3) of the Act, replacing a general reference to a consolidation of regulations to the Consolidated Regulations published in 1978 and any future revision of regulations published under the *Statute Revision Act*[60].

VI. AMENDMENTS TO THE *STATUTE REVISION ACT*

IT MAY SEEM DIFFICULT to relate amendment of the *Statute Revision Act* to an electronic commerce initiative but they are related. The sections in Part 5[61] amend a piece of legislation originally enacted in 1974. The purpose of the statute is to provide for the continuing revision and consolidation of statutes and regulations of Canada, to be done by the Statute Revision Commission.[62] The Consolidated Regulations, published in 1978, and the Revised Statutes, produced in 1985, along with a loose-leaf edition of the Statutes, discontinued in 1993, constitute the efforts of the Commission during its existence. In the early 1990s, the Commission terminated operations and ceased to exist.

Since 1995, the Department of Justice has been making its database of consolidated statutes and regulations available via the World Wide Web. This database is updated three times a year and is unofficial—it cannot be used in evidence for any purpose under the *Canada Evidence Act*.

The demand for knowledge of applicable laws and regulations is growing in an Internet-aware society. Electronic access meets this demand and, in fact, the most popular part of the Department of Justice web site is the section containing federal legislation. One of the themes of the government's electronic commerce initiative is to update the legislative framework to facilitate on-line commerce and government service delivery. As society moves to the increased use of electronic documents, it makes sense, as in the case of an official on-line version of the Canada Gazette, that there be an official electronic version of federal statutes and regulations. The amendments in Part 5 facilitate the production of and access to such a version.

The first amendment is a change in the title of the statute[63] from Statute Revision Act to Legislation Revision and Consolidation Act; the new title more accurately reflecting the nature of the work to be done. The reference to "leg-

---

60 R.S.C. 1985, c. S–20.

61 Bill C–6, *supra* note 3 at s. 60–71.

62 The Commission had three employees of the Department of Justice appointed by the Minister of Justice.

63 Bill C–6, *supra* note 3 at s. 60.

islation" is intended to cover both statutes and regulations. Revision of statutes and regulations is to be done by the Commission[64]; consolidation is to be done by the Minister of Justice[65]. Revision is more than consolidation in that it may involve re-numbering, re-organising and re-writing portions of legislation; consolidation involves the "aggregation" of amendments to a particular piece of legislation into one coherent document, sometimes with grammatical and typographical errors corrected.

Section 68 inserts a new section 21 which permits the Queen's Printer to publish an edition of the Revised Regulations in electronic form and every copy of a revised regulation in electronic form is evidence of the regulation and contents published by the Queen's Printer unless otherwise shown.

Section 71 enacts a completely new Part III containing a new section 26 which authorises the Minister of Justice to maintain a consolidation of both the statutes and regulations of Canada. A new section 28 permits publication in a printed or electronic form in any manner or frequency the Minister considers appropriate

Consolidation statutes and regulations do not operate as new law.[66] However, they do constitute evidence of the statute or regulation in question and its contents.[67]

Where there is an inconsistency between a published version of a statute or regulation and the original statute or regulation, the original version of the statute or regulation prevails to the extent of the inconsistency. Reference is to be made to a copy of the statute or regulation as certified by the Clerk of the Parliaments under the *Publication of Statutes Act*[68] or to a copy of the regulation, as registered by the Clerk of the Privy Council under the *Statutory Instruments Act*.[69] The concern here is with respect to electronic versions of statutes and regulations and an incorrect electronic version being available to the public. As in the case of Part 4, it is anticipated that Part 5 will be proclaimed at a time when the appropriate technology is in place to ensure the integrity of on-line versions of statutes and regulations.

Finally, a new section 32 permits the Minister of Justice to enter into agreements for the publication, sale or distribution of the consolidated statutes or regulations.

---

64 See s. 62 and s. 64, *Ibid.*, which replaces s. 11 and s. 12 with new s. 10 and s. 11.

65 *Ibid.* at s. 71 repeals Part III of the Act and replaces it in its entirety. The Minister's authority to maintain of consolidation of both statutes and regulations is in a new section 26.

66 *Statutory Instruments Act, supra* note 50 at s. 30.

67 *Ibid.* at s. 31(1).

68 R.S.C. 1985, c. S–21.

69 *Statutory Instruments Act, supra* note 50 at ss. 31(2) and 31(3).

VII. CONCLUSION

THE 21ST CENTURY BECKONS. No one knows what life will be like during the next few decades but one thing is sure—the Internet will be a part of it. Perhaps a small part of life for this generation but a larger part for the next one and a still larger one for the generation that follows after it. Governments will have to recognise and assess how this phenomenon affects their citizens.

The ability to accumulate and manipulate personal information dictates a need for sensitivity to the privacy concerns of individual Canadians. Part 1 of Bill C–6 attempts to provide a framework for organisations in Canada to address these privacy concerns – not only on-line but also anywhere personal information is collected or used.

As governments attempt to use new communication tools such as the Internet to deliver services and communicate, there are myriad questions raised about government's legislative authority to use electronic alternatives to paper. Providing for an alternative, acceptable medium is not new. Section 2.1 of the *Public Documents Act* [70] states, in part:

> Unless some Act relating thereto expressly so provides, no commission or other public document...no letters patent of Canada and no public writ, deed or other document thereof...is required to be on parchment but, when written or printed wholly or in part on paper, is as valid in all respects as if written or printed on parchment.

With Parts 2, 4 and 5 the federal government now moves from parchment to paper to electronic media.

Part 3 is intended to remove possible confusion about the admissibility of electronic documents into evidence.

Bill C–6 is an attempt to update federal legislation in response to changes in society that technology has introduced. Given the growing influence of new communication technologies such as the Internet, both policy and law-makers will have to be sensitive to the effect of technology in shaping future legislation.

---

[70] R.S.C. 1985, c. P–28.